Defend what you create

User manual

1992-2014, Doctor Web. All rights reserved

This document is the property of Doctor Web. No part of this document may be reproduced, published or transmitted in any form or by any means for any purpose other than the purchaser's personal use without proper attribution.

TRADEMARKS
Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, Dr.Web AV-Desk and the Dr.WEB logo are trademarks and registered trademarks of Doctor Web in Russia and/or other countries. Other trademarks, registered trademarks and company names used in this document are property of their respective owners.

DISCLAIMER
In no event shall Doctor Web and its resellers or distributors be liable for errors or omissions, or any loss of profit or any other damage caused or alleged to be caused directly or indirectly by this document, the use of or inability to use information contained in this document.

Dr.Web Anti-virus for Linux
Version 9.0.0
User manual
05.05.2014

Doctor Web Head Office
2-12A, 3rd str. Yamskogo polya
Moscow, Russia
125124

Web site: www.drweb.com
Phone: +7 (495) 789-45-87

Refer to the official web site for regional and international office information.

Doctor Web

Doctor Web develops and distributes Dr.Web® information security solutions which provide efficient protection from malicious software and spam.

Doctor Web customers can be found among home users from all over the world and in government enterprises, small companies and nationwide corporations.

Dr.Web antivirus solutions are well known since 1992 for continuing excellence in malware detection and compliance with international information security standards. State certificates and awards received by the Dr.Web solutions, as well as the globally widespread use of our products are the best evidence of exceptional trust to the company products.

We thank all our customers for their support and devotion to the Dr.Web products!

Table of Contents

Document Conventions 6

Introduction 7

About this Product 8

- **Main Functions** 8
- **System Requirements** 9
- **Program Structure** 10
- **Quarantine directories** 10
- **Files Permissions and Privileges** 11
- **Operation Modes** 11
- **Testing Anti-virus Operation** 14

Licensing 15

- **Key File** 17
- **Connection Settings File** 18

Installing and Removing Dr.Web Anti-virus for Linux 19

- **Upgrading to Newer Version** 19
- **Installation Procedure** 20
  - Installing Universal Package 20
    - Installing in Graphics Mode 21
    - Installing from Command Line 25
  - Installing from Dr.Web Repository 28
  - Adjusting SELinux Policies 29
  - Product Files Location 31
- **Removing Dr.Web Anti-virus for Linux** 32
  - Removing Universal Package 32
    - Removing in Graphics Mode 32
    - Removing from Command Line 34
  - Removing Product Installed from Repository 37

Working with Dr.Web Anti-virus for Linux 39

- **Operating in Graphics Mode** 39
  - Starting and Shutting Down Graphical Interface 42
  - Indicator in desktop tray 42
  - Threat Detection and Neutralization 43
    - Scanning on Demand 44

Managing Scan Tasks 46
Monitoring File System 49
Viewing Detected Threats 50
Managing Quarantine 52
Updating Virus Databases 54
License Manager 55
Managing Application Privileges 64
Help and Reference 65
Configuring Operation Settings 66
Main Settings 66
Scanner Settings 68
SpIDer Guard Settings 69
Exclusions 70
Scheduler Settings 71
Mode Settings 72
Advanced 75
Command Line Parameters 75
Working from Command Line 75
Call Format 76
Example Usage 84
Appendicies 86
Appendix A. Types of Computer Threats 86
Appendix B. Fighting Computer Threats 90
Appendix C. Contacting Support 92
Index 93

Document Conventions

The following conventions and symbols are used in this manual:

Convention	Description
Bold	Names of buttons and other elements of the graphical user interface (GUI), and required user input that must be entered exactly as given in the guide.
Green and bold	Names of **Dr.Web** products and components.
Green and underlined	Hyperlinks to topics and webpages.
`Monospace`	Code examples, input to the command line and application output.
Italic	Placeholders which represent information that must be supplied by the user. For command-line input, it indicates parameter values. In addition, it may indicate a term in position of a definition.
CAPITAL LETTERS	Names of keys and key sequences.
Plus sign ('+')	Indicates a combination of keys. For example, ALT+F1 means to hold down the ALT key while pressing the F1 key.
	A warning about potential errors or any other important comment.

Introduction

Thank you for purchasing **Dr.Web® Anti-virus for Linux** (hereinafter **Dr.Web Anti-virus for Linux**). It offers reliable protection from various types of computer threats using the most advanced virus detection and neutralization technologies.

This manual is intended to help users of computers running under OS **GNU/Linux** family (**Linux** hereinafter) install and use **Dr.Web Anti-virus for Linux** 9.0.0.

If **Dr.Web Anti-virus for Linux** 6.0.2 is already installed on you computer and you wish to upgrade **Anti-virus** to version 9.0.0, do the steps of the upgrade procedure.

About this Product

Dr.Web Anti-virus for Linux is an anti-virus solution designed to protect computers running under OS **GNU/Linux** family from viruses and threats of other types.

The core components of the program (anti-virus engine **Dr.Web Virus-Finding Engine** and **Dr.Web** virus databases) are not only extremely effective and resource-sparing, but also cross-platform, which allows **Dr.Web** specialists to create outstanding anti-virus solutions for different operating systems.

Components of **Dr.Web Anti-virus for Linux** are constantly updated and virus databases are supplemented with new signatures to assure up-to-date protection. Moreover, heuristic analysis methods are used for providing additional protection against unknown viruses.

Main Functions

Dr.Web Anti-virus for Linux provides you with the following features:

1. **Detection and neutralization** of malicious programs (for example, viruses, including those that infect mailboxes and boot records, Trojan programs, mail worms) and unwanted software (for example, adware, joke programs, dialers).

   Dr.Web Anti-virus for Linux uses several malicious software detection methods simultaneously:

   - *signature analysis* which allows detection of known threats
   - *heuristic analysis* which allows detection of threats that are not present in virus databases.

   Note that as with any system of hypothesis testing under uncertainty, the *heuristics analyzer* may omit viruses or raise false alarms. As an object can be erroneously considered as malicious, all threats detected by the *heuristics analyzer* are treated as suspicious. So, it is recommended not to delete such threats but move them to **Quarantine** and send to **Doctor Web Virus Laboratory** for analysis. For details on methods to neutralize computer threats, refer to Fighting computer Threats (Appendix B).

   System objects are scanned at user request or automatically, according to the scheduled. The user can launch scanning of all file system objects (including both files and boot records) as well as select custom scan when only specified files, directories, and boot records are scanned. Also it is possible to launch scanning only of binary executable files containing code of currently running processes. If a threat is detected in such case, not only the malicious object is neutralized but also the active process is terminated.

2. **Monitoring access to data files and attempts to run executables**. This feature allows detection and neutralization of malware right at the moment of an infection attempt.
3. **Reliable isolation of infected or suspicious objects**. Such objects are moved to a special storage, **Quarantine**, to prevent any harm to the system. When moving to **Quarantine**, objects are renamed according to special rules and, if necessary, they can be restored to their original location only at user request.
4. **Automatic update** of **Dr.Web** virus databases and anti-virus engine to enable **Anti-virus** to use the most recent information about known malicious software.
5. **Operation in central protection mode** (when connected to the central protection server, such as **Dr.Web Enterprise Server** or as a part of **Dr.Web AV-Desk** service). This mode allows to implement a unified security policy on the computers of the protected network. It can be a corporate network, a private network (VPN), or a network of a service provider (for example, a provider of Internet service) .

System Requirements

You can use **Dr.Web for Linux Anti-virus** on a computer that meets the following requirements:

Specification	Requirement
Platform	Both 32-bit **(IA-32, x86)** and 64-bit **(x86-64, x64, amd64) Intel** platforms are supported.
Hard disk space	Minimum 400 MB of free disk space on a volume where the **Anti-virus** directories are located.
OS	**Linux** for **Intel x86/amd64** platform based on **kernel** ver. 2.6.37 or later, and using library **glibc** ver. 2.13 or later. Tested **Linux** distributions are listed below. On systems operating on 64-bit platform, support of 32-bit applications must be enabled (probably, additional libraries must be installed for it, see below).
Other	The following valid network connections: Valid Internet connection to enable updates for virus databases and **Dr.Web for Linux** components. When operating in central protection mode, connection to the server in the network is enough; connection to the Internet is not required.

The product was tested on the following **Linux** distributions (32-bit and 64-bit):

Linux distribution name	Version	Required additional libraries for 64-bit OS version
Debian	7	**libc6-i386**
Fedora	20	**glibc.i686**
Mint	16	**libc6-i386**
Ubuntu	12.04 LTS, 13.04, 13.10, 14.04	**libc6-i386**

Other **Linux** distributions that meet the above-mentioned requirements have not been tested for compatibility with the **Anti-virus** but may be supported. If a compatibility issue occurs, contact Technical support on the official website at http://support.drweb.com/request/.

Additional Packages

- To enable **Anti-virus** operation in graphics mode and startup of the program for product installation and removal in graphics mode, **X Window System** graphics subsystem and any window manager is required. Moreover, for correct operation of indicator for **Ubuntu Unity** desktop environment, the **libappindicator1** library is also required.
- To start the product installer or uninstaller, designed for the command line, in graphics mode, a terminal emulator (such as **xterm**, **xvt**, etc.) is required.
- The following additional packages and tools must be installed in the operating system: **unzip**, **crond**. To enable privilege elevation, the **su** or **sudo** utilities and the **xterm** terminal emulator are required. Instead of this, it is recommended to install one of the utilities for elevating privileges from the desktop environment: **gksu**, **gksudo**, **kdesu**, **kdesudo**, **beesu**, **beesudo**.

For convenient work with **Anti-virus** in the command line, you can enable command auto-completion in the used command shell (if disabled).

If you encounter any problem with installation of additional packages and components, refer to User Manuals for the used distribution of the operating system.

Program Structure

Dr.Web Anti-virus for Linux consists of the following components:

Component	Description
Scanner	Scans file system objects (files, directories, and boot records) for threats. Scanning can be started at user request or as scheduled. The user can start scanning from both graphics and command-line modes.
SpIDer Guard file system monitor	Operates in resident mode and monitors file system operations (such as creation, opening, and closing a file). Sends **Scanner** requests to check contents of new or modified files and contents of executables when they are attempted to run.
Anti-virus engine	Central component of anti-virus protection used by **Scanner** for searching and detecting of threats as well as for analysis of suspicious object behavior.
Virus databases	Automatically updated database used by the anti-virus engine and containing information for detection and neutralization of known threats.
Updater	Downloads updates to the virus databases and anti-virus engine from **Dr.Web GUS** servers automatically, according to the schedule or at user request.
Quarantine	The component which provides a special storage used by **Anti-virus** isolation of malicious and suspicious files to prevent them from doing any harm to the system.
License manager	Helps users manage their licenses and do the following: activate a license and demo period, view information on the current license, renew the license, as well as install or remove a license key file.

Apart from the components described in the table, **Dr.Web Anti-virus for Linux** includes service components that operate in the background mode and do not require user intervention.

Quarantine directories

Quarantine directory serves for isolation of files that pose a threat to system security and cannot be currently cured. Such threats are those that are unknown to **Anti-virus** (that is, a virus is detected by the *heuristic analyzer* but the virus signature and method to cure are absent in the databases) or those that cause an error during scanning. Moreover, a file can be quarantined at user request if the user selected this action in the list of detected threats or specified this action in **Scanner** or **SpIDer Guard** settings as reaction to this threat type.

When a file is quarantined, it is renamed according to special rules. Renaming of isolated files prevents users and applications from accessing these files in case of bypassing **Quarantine** management tools implemented in **Dr.Web Anti-virus for Linux.**

Quarantine directories are located in

- **user home directory** (if multiple user accounts exist on the computer, a separate **Quarantine** directory can be created for each of the users).
- **root directory** of each logical volume mounted to the file system.

Dr.Web Quarantine directories are always named as `.com.drweb.quarantine` and are not created until the `Quarantine (Isolate)` action is applied. At that, only a directory required for isolation of a concrete object is created. When selecting a directory, the file owner name is used: search is performed upwards from the location where the malicious object resides and if the owner

home directory is reached, the **Quarantine** storage created in this directory is selected. Otherwise, the file is isolated in the quarantine created in the root directory of the volume (which is not always the same as the file system root directory). Thus, any infected file moved to **Quarantine** always resides on the volume, which allows for correct operation of **Quarantine** in case several removable data storages and other volumes are mounted to different locations in the system.

Users can manage objects in **Quarantine** both in graphics mode and from the command line. Every action is applied to the consolidated **Quarantine**; that is, changes affect all **Quarantine** directories available at the moment. From the viewpoint of the user, the **Quarantine** directory located in the user home directory is considered *User Quarantine* and other directories are considered *System Quarantine*.

Operation with quarantined objects is allowed even if no active license is found. However, isolated objects cannot be cured in this case.

Files Permissions and Privileges

To scan objects of the file system and neutralize threats, **Dr.Web Anti-virus for Linux** (or rather the user **Anti-virus** runs under) requires the following permissions:

Action	Required permissions
Listing all detected threats	Unrestricted. No special permission required.
List archive contents (only corrupted or malicious elements)	Unrestricted. No special permission required.
Moving to **Quarantine**	Unrestricted. A user can quarantine all infected files regardless of read or write permissions on them.
Removing a threat	User must have write permission on the deleted file.
Curing	Unrestricted. The permissions and owner of a cured file remain the same. If deletion is applied to the file while curing, it is removed from the system regardless of the permissions that the user has on the file.
Restoring a file from **Quarantine**	User must have permissions to read the file and to write to the restore directory.
Deleting a file from **Quarantine**	User must have write permissions to the file that was moved to **Quarantine.**

To temporarily elevate **Dr.Web Anti-virus for Linux** privileges in graphics mode, click the corresponding button on the **Anti-virus** window. To enable operation of the **Anti-virus** in graphics mode or of the command-line management tool with superuser privileges, you can use the `su` command, which allows to change the user, or the `sudo` command, which allows to execute a command as another user.

Note that **Scanner** cannot check file which size exceeds 4 Gbytes (on attempt to scan such files, the following error message displays: "File too large").

Operation Modes

Dr.Web Anti-virus for Linux can operate both in Standalone mode and as a part of an anti-virus network managed by a central protection server. Operation in Central protection mode does not require installation of additional software or **Dr.Web Anti-virus for Linux** reinstallation or removal.

- **In Standalone mode**, the protected computer is not connected to an anti-virus network and its operation is managed locally. In this mode, configuration and license key files reside on local disks and **Dr.Web Anti-virus for Linux** is fully controlled from the protected computer. Updates to virus

databases are received from **Dr.Web GUS** servers.

- **In Central Protection mode**, protection of the computer is managed by the central protection server. In this mode, some functions and settings of **Dr.Web Anti-virus for Linux** can be adjusted in accordance with the general (corporate) anti-virus protection policy implemented in the anti-virus network. The license key file used for operating in Central protection mode is received from the central protection server. The key file stored on the local computer, if any, is not used. Statistics on virus events is sent to the central protection server. Updates to virus databases are also received from the central protection server.
- **In Mobile mode**, **Dr.Web Anti-virus for Linux** receives updates from the **Dr.Web GUS** servers, but operation of **Anti-virus** is managed with the local settings. The used key file is received from the central protection server.

When **Anti-virus** is operating in Central protection or Mobile mode, the following options are blocked:

1. Deletion of a license key file in **License Manager**;
2. Manual start of an update process and adjustment of update settings;
3. Configuration of file system scanning parameters.

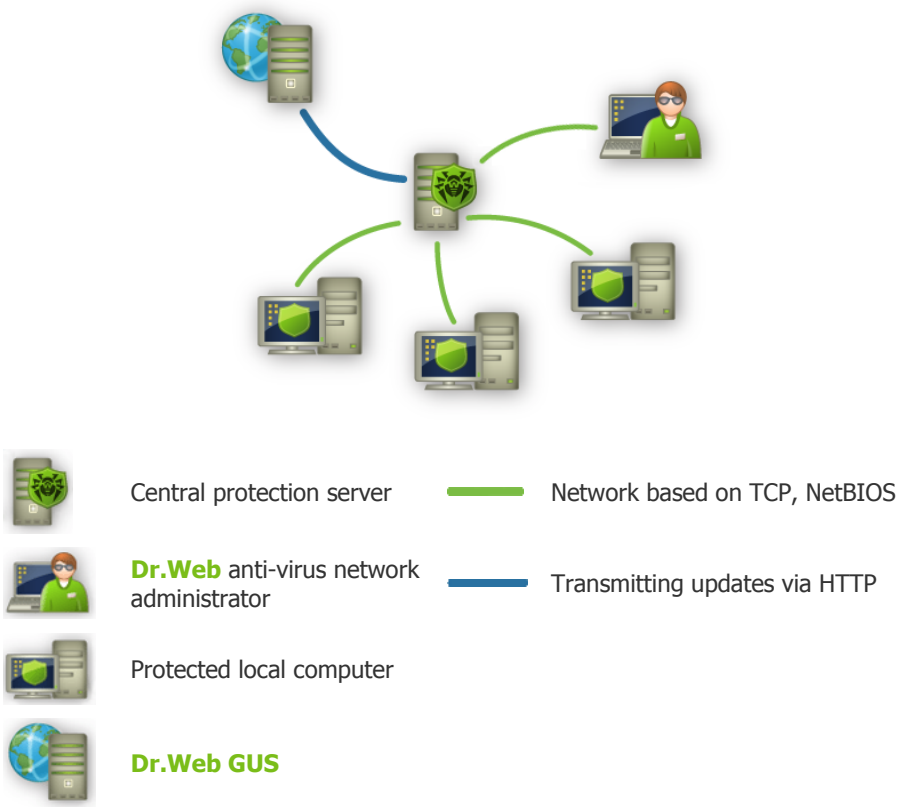
Configuration of **SpIDer Guard** settings as well as an option to enable or disable **SpIDer Guard** checks are allowed in dependence on permissions specified on the server.

Note that if launch of scanning at user request is prohibited on the used central protection server, the Scan page of the **Anti-virus** window will be disabled. Moreover, in this case the **Scheduler** will not launch scans even if they are scheduled.

Logical Structure of Anti-Virus Networks

Doctor Web solutions for central protection use client-server model (see the picture below).

Workstations and servers are protected by *local anti-virus components* (herein, **Dr.Web Anti-virus for Linux**) installed on them, which provides for anti-virus protection of remote computers and allows connection between the workstations and the central protection server.



Picture 1. Logical structure of the Anti-Virus Network

Local computers are updated and configured from the *central protection server*. The stream of instructions, data and statistics in the anti-virus network goes also through the central protection server. The volume of traffic between protected computers and the central server can be quite sizeable, therefore solutions provide options for traffic compression. To prevent leak of sensitive data or substitution of software downloaded onto protected computers, encryption is also supported.

All necessary updates are downloaded to the central protection server from **Dr.Web GUS**.

Local anti-virus components are configured and managed from the central protection server according to commands from anti-virus network administrators. Administrators manage central protection servers and topology of anti-virus networks (for example, validate connections to the central protection server from remote computers) and configure operation of local anti-virus components when necessary.

Local anti-virus components are not compatible with anti-virus products of other companies or anti-virus solutions of **Dr.Web** if the latter do not support operation in Central protection mode (for example, version 5.0 of **Dr.Web Anti-virus for Linux**). Installation of two anti-virus programs on the same computer can cause a system crash and loss of important data.

Connecting to Anti-Virus Network

Dr.Web Anti-virus for Linux can be connected to an anti-virus network in one of the following ways:

- During **Dr.Web Anti-virus for Linux** activation – in the **License Manager**
- On the **Mode** tab of the settings window in the **Dr.Web Anti-virus for Linux** graphical interface
- Using the `esconnect` command of the command-line management tool – **`drweb-ctl`**

If **Dr.Web Anti-virus for Linux** is a part of the anti-virus network, you can switch **Anti-virus** operation between Mobile and Central protection modes. For that purpose, use the `esmobile` command of the command-line management tool – **`drweb-ctl`**.

Disconnecting from Anti-Virus Network

Dr.Web Anti-virus for Linux can be disconnected from the anti-virus network in one of the following ways:

- On the **Mode** tab of the settings window in the **Dr.Web Anti-virus for Linux** graphical interface
- Using the `esdisconnect` command of the command-line management tool – **`drweb-ctl`**

Testing Anti-virus Operation

The `EICAR` (*European Institute for Computer Anti-Virus Research*) Test helps testing performance of anti-virus programs that detect viruses using signatures. This test was designed specially so that users could test reaction of newly-installed anti-virus tools to detection of viruses without compromising security of their computers.

Although the `EICAR` test is not actually a virus, it is treated by the majority of anti-viruses as if it were a virus. On detection of this "virus", **Dr.Web** anti-virus products report the following: **`EICAR Test File (Not a Virus!)`**. Other anti-virus tools alert users in a similar way. The `EICAR` test file is a 68-byte COM-file for MS DOS/MS Windows OS that outputs the following line on the console when executed:

```
EICAR-STANDARD-ANTIVIRUS-TEST-FILE!
```

The `EICAR` test contains the following character string only:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

To create your own test file with the "virus", you may create a new file with the line mentioned above.

If **Dr.Web Anti-virus for Linux** operates correctly, the `EICAR` test file is detected during a file system scan regardless of the scan type and the user is notified on the detected threat: **`EICAR Test File (Not a Virus!)`**.

Licensing

Permissions to use **Dr.Web Anti-virus for Linux** are granted by the *license* purchased from **Doctor Web** company or from **Doctor Web** partners. License parameters determining user rights are set in accordance with the **License agreement** which the user accepts during product installation. The license agreement contains information on the user and the vendor as well as usage parameters of the purchased product, including:

- list of components licensed to the user;
- license period;
- other restrictions (for example, number of computers on which the purchased **Anti-virus** is allowed for use).

For evaluation purposes users may also activate *demo period*. After successful activation, demo period provides users with full functionality of the solution for the whole activated period.

Each **Doctor Web** product license has a unique serial number associated with a special file stored on the user computer. This file regulates operation of the **Anti-virus** components in accordance with the license parameters and is called a *license* key file. Upon activation of a demo period, a special key file, named a *demo* key file, is automatically generated.

If a license or a demo period are not activated on the computer, the **Anti-virus** components are blocked. Moreover, updates to virus databases cannot be downloaded from **Dr.Web Global Update System** (**Dr.Web GUS**). But you can activate **Anti-virus** by connecting it to the central protection server as a part of the anti-virus network administered by the enterprise or Internet service provider. In this case, operation of **Anti-virus** and updating are managed by the central protection server.

Purchasing and Registering Licenses

After a license is purchased, updates to product components and virus databases are regularly downloaded from **Dr.Web GUS**. Moreover, if the customer encountered any issue when installing or using the purchased product, they can take advantage of Technical Support service provided by **Doctor Web** or **Doctor Web** partners.

You can purchase any **Dr.Web** product as well as obtain a product serial number either on the online store or from our partners. For details on license periods and license types, visit the **Doctor Web** official website at http://www.drweb.com/.

License registration is required to prove that you are a legal user of **Dr.Web Anti-virus for Linux** and activate **Anti-virus** functions including virus database updating. It is recommended to register the product and activate the license once installation completes. A purchased license can be activated in one of the following ways:

- via the Registration Wizard included in **License Manager**.
- on the **Doctor Web** official website at http://products.drweb.com/register/.

During activation, it is required to enter the serial number of the purchased license. The serial number is supplied with the product or via email when purchasing or renewing the license online.

If you have used **Dr.Web Anti-virus for Linux** in the past, you may be eligible for a 150-day extension to your new license. To enable the bonus, enter your registered serial number or provide the license key file. Otherwise, if you select an option to renew the license but do not provide the previous license data, the period of license validity will be reduced by 150 days.

If you have several licenses for using **Anti-virus** on several computers, but choose to use the product only on one computer, you can specify this and, hence, license validity period will be automatically extended.

Obtaining Demo License

Users of **Dr.Web** can obtain a demo period for

- 3 months
- 1 month

To obtain a demo period for 3 months, register on the **Doctor Web** official website and provide the requested personal data. After registration completes, you will receive an email with a serial number for **Anti-virus** activation. Demo period for 1 month can be received in the Registration wizard window of **License Manager**. To obtain a demo period for 1 month, you do not need to provide your personal data.

You can start registration or obtain a demo period from the **License Manager** window at any time by clicking the **Activate License** button on the page with information on the current license.

To activate a license using the serial number or request a demo license, a valid Internet connection is required.

Demo period for the same computer cannot be obtained more often than once a year.

When a demo period or license is activated via **License Manager**, the key file (license or demo) is automatically generated on the local computer in its target directory. If you register on the website, the key file is sent by email and you need to install the key file manually.

Subsequent Registration

If a key file is lost but the existing license is not expired, you must register again by inputting the personal data you provided during the previous registration. You may use a different email address. In this case, the key file will be sent to the newly specified address.

The number of times you can request a key file is limited. One serial number can be registered no more than 25 times. If requests in excess of that number are sent, no key file will be delivered. To receive a lost key file, contact Technical Support, describe your problem in detail, and state personal data you entered upon serial number registration. The license key file will be sent by email.

Key File

Key file is a special file stored on the local computer. It corresponds to the purchased license or activated demo period for **Dr.Web Anti-virus for Linux**. The file contains information on the provided license or demo period and regulates usage rights in accordance with it.

The key file has `.key` extension and is valid if satisfies the following criteria:

- license or demo period is not expired;
- demo period or license applies to all anti-virus components required by the product;
- integrity of the key file is not violated.

If any of the conditions are violated, the license key file becomes invalid.

During **Dr.Web Anti-virus for Linux** operation, the key file must reside in the default `/etc/opt/drweb.com` directory and have the **`drweb32.key`** name.

Components of **Anti-virus** regularly check whether the key file is available and valid. The key file is digitally signed to prevent its editing. So, the edited key file becomes invalid. It is not recommended to open your key file in text editors in order to avoid its accidental invalidation.

If no valid key file (license or demo) is found, or if the license is expired, operation of the anti-virus components is blocked until a valid key file is installed.

It is recommended to keep the license key file until it expires, and use it to reinstall **Dr.Web Anti-virus for Linux** or install it on a different computer. In this case, you must use the same product serial number and customer data that you provided during the registration.

Key File Installation

If you have a key file corresponding to the valid license for the product (for example, if you obtained the key file by email or if you want to use **Dr.Web Anti-virus for Linux** on another computer), you can activate **Anti-virus** by specifying the path to the key file.

You can specify the key file path

- in the **License Manager** by clicking **Other activation types** on the first step of the registration procedure and specifying the key file path.
- manually. For that purpose
  1. unpack the key file if archived;
  2. copy the file to the `/etc/opt/drweb.com` directory and rename it to **`drweb32.key`**

You can also use the following command:

```
$ drweb-ctl cfset Root.KeyPath </path/to/key/file>
```

In this case, the key file will not be copied to the `/etc/opt/drweb.com` directory and will remain in its original location. If so, the user becomes responsible for ensuring that the file is protected from corruption or deletion. This installation method is not recommended as the key file can be accidentaly deleted from the system (for example, if the directory, where the key file resides, is periodically cleaned up).

Connection Settings File

The connection settings file is a special file that stores parameters that configure connection between **Dr.Web Anti-virus for Linux** and the central protection server.

This file is supplied by the administrator of the Anti-virus network or the Internet service provider (if the latter provides support for the central anti-virus protection service).

You can use this file to activate **Dr.Web Anti-virus for Linux** when connecting it to the central protection server (in this case, you cannot use **Anti-virus** in Standalone mode without purchasing additional license).

Activation via Connection to Central Protection Server

If the Internet service provider or network administrator submitted a file with settings of connection to the central protection server, you can activate **Anti-virus** by specifying the file path.

To specify a path to the connection settings file

- open **License Manager** and start the registration procedure by clicking the **Activate license** button;
- select the **Other activation types** option;
- specify the file path in the displayed entry field.

Installing and Removing Dr.Web Anti-virus for Linux

This section describes how to install, update, and remove **Dr.Web Anti-virus for Linux** of version 9.0.0. Also in this chapter you can find the procedure of updating to a new version, if **Dr.Web Anti-virus for Linux** of version 6.0.2 is already installed on your computer.

These procedures can be performed only by a user with administrative privileges (`root` superuser). To elevate privileges, use the **su** command (change the current user) or the **sudo** command (execute the specified command with other user privileges).

Upgrading to Newer Version

If you use **Dr.Web Anti-virus for Linux** 6.0.2 and wish to upgrade it to version 9.0.0, reinstall the product.

Please note that updating to a new version of **Anti-virus** should be performed the same way as was used at installation of **Anti-virus** 6.0.2:

- If the previous version is installed from the repository, then it is recommended to perform updating to a new version by updating a version from the repository.
- If the previous version is installed from the distribution, then updating should be performed by installation of a distribution which contains a new version.

If you cannot update the product the way you installed it initially, remove **Dr.Web Anti-virus for Linux** 6.0.2, and then perform an installation of a new version using the convenient method. Installation and removal of **Dr.Web Anti-virus for Linux** 6.0.2 are the same as installation and removal, that are described in this manual for version 9.0.0. For additional information, see User manual for **Dr.Web Anti-virus for Linux** 6.0.2.

- When installing **Dr.Web Anti-virus for Linux** 9.0.0 from the installation file, you are prompted to automatically remove the older version installed from the distribution.
- For updating of **Dr.Web Anti-virus for Linux** 6.0.2 installed from the **Doctor Web** repository, do the following:
  - change the used repository (from the package repository 6.0.2 to the package repository 9.0. You can find the name of the repository in the Installing from Dr.Web Repository chapter);
  - update the product. For this, use the following commands:

    In case of using RPM packets:

    ```
    # yum update
    ```

    In case of using DEB packets:

    ```
    # apt-get update
    # apt-get dist-upgrade
    ```

Regardless of the selected method to upgrade **Anti-virus**, the license key file is installed to the default location (the new version uses the key file either while operation of the installation wizard or on the first **Anti-virus** startup in graphics mode).

If any problem occurs during automatic installation of the key file, you can install it manually. The license key file of **Dr.Web Anti-virus for Linux** 6.0.2 resides in the `/home/<user>/.drweb` directory (the directory is hidden).

If a valid license key file is lost, contact **Doctor Web** Technical support.

Dr.Web Anti-virus for Linux 9.0.0 does not support **Quarantine** of **Dr.Web Anti-virus for Linux** 6.0.2! If any isolated files remain in **Quarantine** of an older version, you can retrieve or delete these files manually. **Quarantine** of **Dr.Web Anti-virus for Linux** 6.0.2 isolates files into the following directories:

- `/var/drweb/infected` – system;
- `/home/<user>/.drweb/quarantine` – user (where `<user>` is the name of the user).

To simplify processing of quarantined files, it is recommended to revise **Quarantine** using **Dr.Web Anti-virus for Linux** 6.0.2 before starting an upgrade.

Note that if **Dr.Web Anti-virus for Linux** 6.0.2 is active when upgrading the product, processes of the older version **remain running until the user logs off the system** after the upgrade is complete. At that, if **Anti-virus** is operating in graphics mode, the icon of the older version can display in the tray.

Installation Procedure

To install **Dr.Web Anti-virus for Linux**, do one of the following:

1. Download the installation file with the universal package for UNIX systems from the **Doctor Web** official website. The package is supplied with installers (both graphical and console) started depending on the environment.
2. Download the native packages from the corresponding package repository of **Doctor Web**.

Regardless of the selected way to install **Dr.Web Anti-virus for Linux**, after the installation completes, you need either to activate the license, or install the key file if obtained, or connect **Anti-virus** to the central protection server.

Until you do that, **anti-virus protection is disabled.**

Installing Universal Package

Dr.Web Anti-virus for Linux is distributed as an installation file named **`drweb-workstations_<version>~linux_<platform>.run`**, where **`<version>`** is a line that contains the version and data of product release, and **`<platfrom>`** is a platform for which the product is intended (**`x86`** for 32-bit platforms and **`amd64`** for 64-bit platforms). For example:

```
drweb-workstations_9.0.0.0-1404011200~linux_x86.run
```

Note that the installation file name corresponding the above-mentioned format is referred to as **`<file_name>.run`**.

To install **Dr.Web Anti-virus for Linux** components automatically

1. download the archive from the official **Doctor Web** website;
2. save the archive to the hard disk drive of the computer;
3. allow the archive to execute, for example, using the following command:

   ```
   # chmod +x <file_name>.run
   ```

4. execute the archive using the following command:

   ```
   # ./<file_name>.run
   ```

   or use the standard file manager of the graphical shell for both changing file properties and running the file.

At that, a `<file_name>` directory with a set of files is created and installation procedure is automatically started. If not started with `root` privileges, the Installation Wizard attempts to elevate the privileges.

Depending on the environment where the distribution is started, one of the following installation programs runs:

- Installation Wizard for graphics mode;
- installer for command-line mode.

At that, the installer for command-line mode is automatically started if the Installation Wizard for graphics mode fails to start.

5. Follow the prompts of the installer.

Note that if the used **Linux** distribution features **SELinux**, the installation process can be interrupted by the security subsystem. If such situation occurs, set **SELinux** to the `(Permissive)` mode. To do this, enter the following command:

```
# setenforce 0
```

and restart the installer.

After the installation completes, configure **SELinux** security policies to enable correct operation of the **Anti-virus** components.

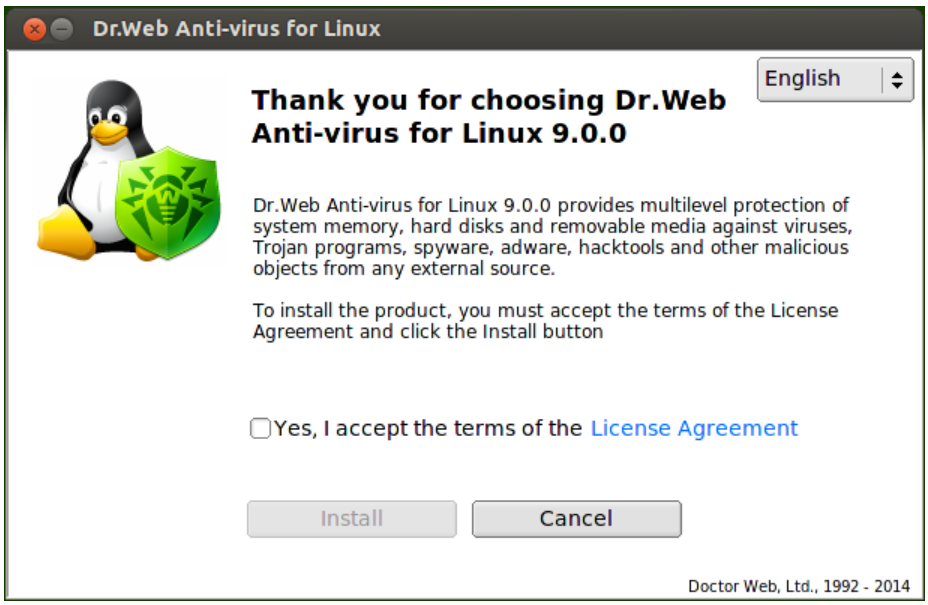
After installation in the desktop graphical shell completes, the **Dr.Web** item displays on the application menu. This item contains two items:

- **Dr.Web for Linux** item to run **Anti-virus Dr.Web for Linux** in graphics mode;
- **Remove Dr.Web components** item to delete the components.

After successful installation you can remove the `<file_name>` directory with installation files.

Installing in Graphics Mode

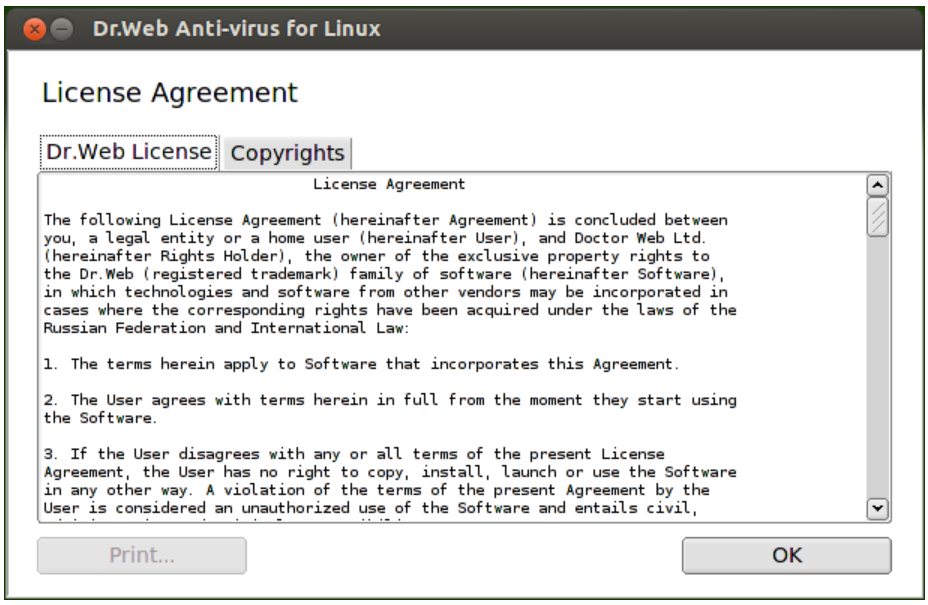
After the installation program for graphics mode starts, a window of the Installation Wizard displays. On the welcome page, you can select the installation language in the drop-down list in the upper-right corner.


Dr.Web Anti-virus for Linux
English
Thank you for choosing Dr.Web Anti-virus for Linux 9.0.0
Dr.Web Anti-virus for Linux 9.0.0 provides multilevel protection of system memory, hard disks and removable media against viruses, Trojan programs, spyware, adware, hacktools and other malicious objects from any external source.
To install the product, you must accept the terms of the License Agreement and click the Install button
Yes, I accept the terms of the License Agreement
Install
Cancel
Doctor Web, Ltd., 1992 - 2014

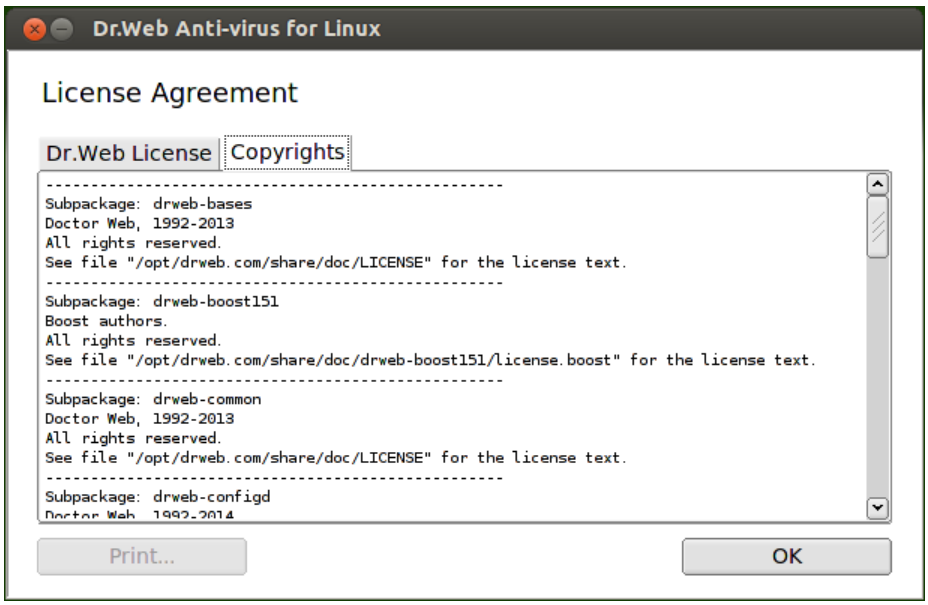
Picture 2. Welcome page

To install **Dr.Web Anti-virus for Linux** on your computer, do the following:

1. View the terms of the **Doctor Web** **License agreement**. For that purpose, click the **Yes, I accept the terms of the License Agreement** link. A page with the text of the **License agreement** and information on the copyright for the components to be installed opens.


Dr.Web Anti-virus for Linux
License Agreement
Dr.Web License
Copyrights
License Agreement
The following License Agreement (hereinafter Agreement) is concluded between you, a legal entity or a home user (hereinafter User), and Doctor Web Ltd. (hereinafter Rights Holder), the owner of the exclusive property rights to the Dr.Web (registered trademark) family of software (hereinafter Software), in which technologies and software from other vendors may be incorporated in cases where the corresponding rights have been acquired under the laws of the Russian Federation and International Law:
1. The terms herein apply to Software that incorporates this Agreement.
2. The User agrees with terms herein in full from the moment they start using the Software.
3. If the User disagrees with any or all terms of the present License Agreement, the User has no right to copy, install, launch or use the Software in any other way. A violation of the terms of the present Agreement by the User is considered an unauthorized use of the Software and entails civil,
Print...
OK

Picture 3. License Agreement page

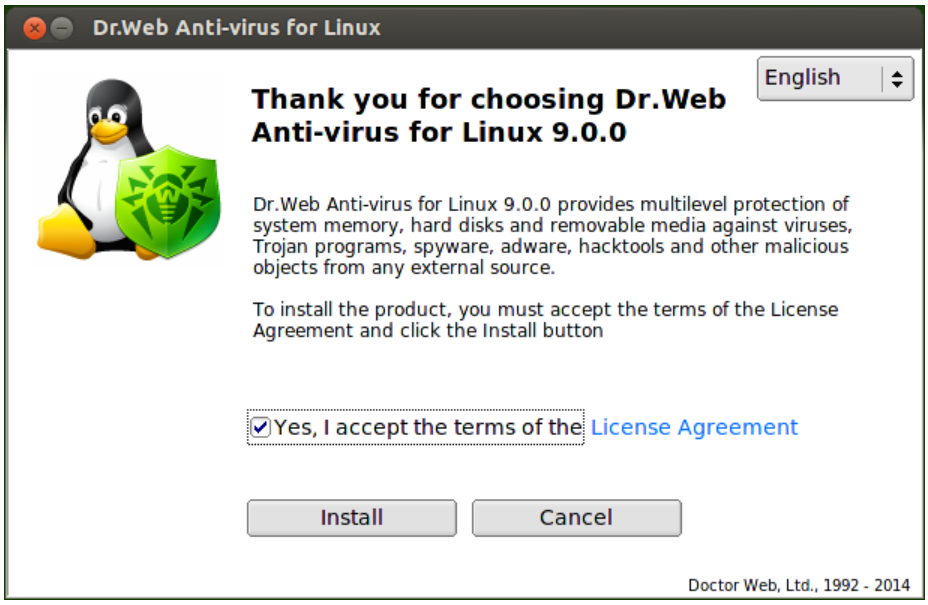


Picture 4. Copyright information page

When required, if a printer is installed and configured in your system, you can print off the **License agreement** terms and copyright information. To do that, open the corresponding tab of the **License agreement** page and click the **Print...** button.

To close the page, click **OK**.

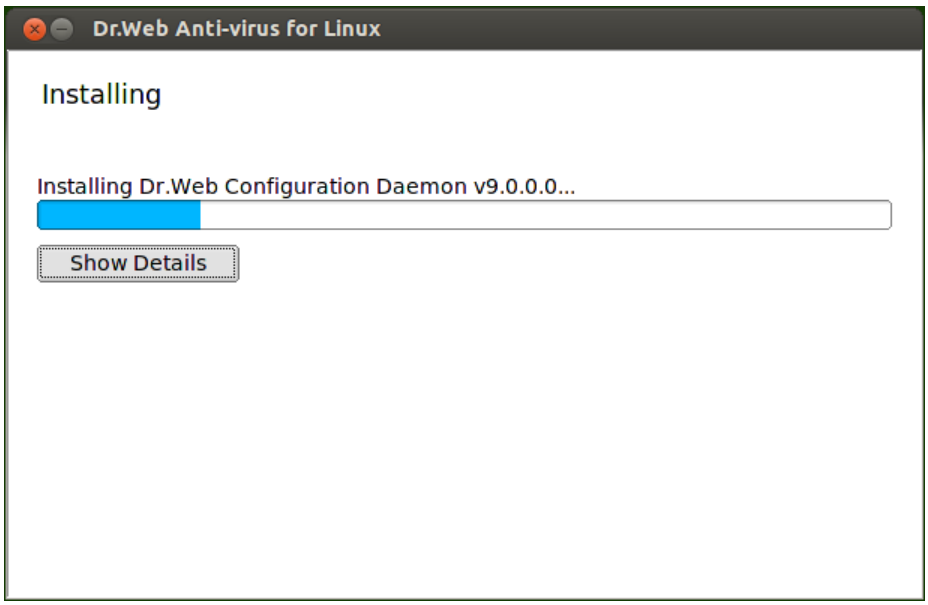
2. To start installation, accept the **Doctor Web** **License agreement** by selecting the **Yes, I accept the terms of the License Agreement** checkbox.


Dr.Web Anti-virus for Linux
English
Thank you for choosing Dr.Web Anti-virus for Linux 9.0.0
Dr.Web Anti-virus for Linux 9.0.0 provides multilevel protection of system memory, hard disks and removable media against viruses, Trojan programs, spyware, adware, hacktools and other malicious objects from any external source.
To install the product, you must accept the terms of the License Agreement and click the Install button
Yes, I accept the terms of the License Agreement
Install
Cancel
Doctor Web, Ltd., 1992 - 2014

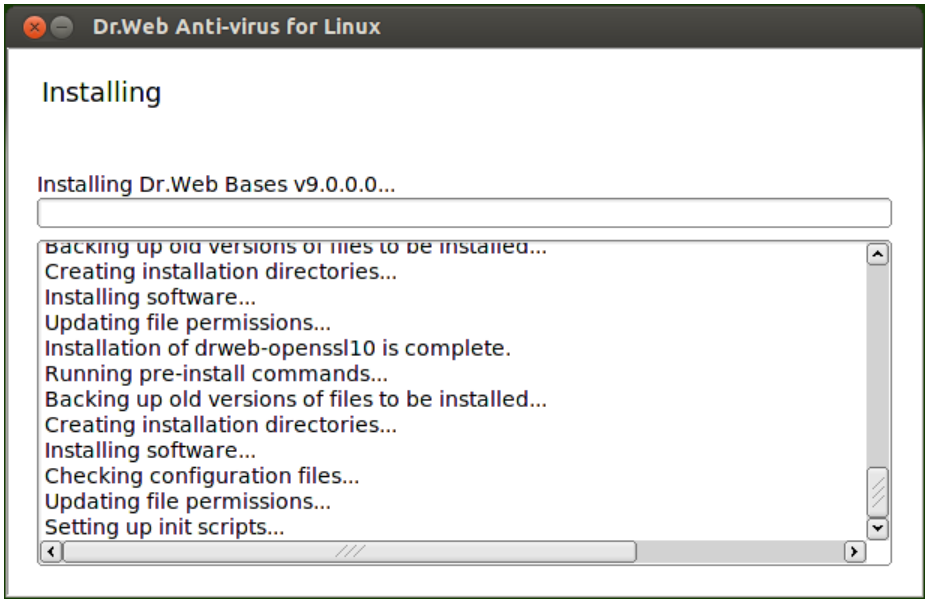
Picture 5. Confirmation of License agreement acceptance

If you choose not to install **Anti-virus** on your computer, click **Cancel**. Once the button is clicked, the Installation Wizard exits. If you choose to install the product, click **Install**.

3. After installation starts, a page with the progress bar opens. If necessary, you can click **Show Details** and view the installation log file.

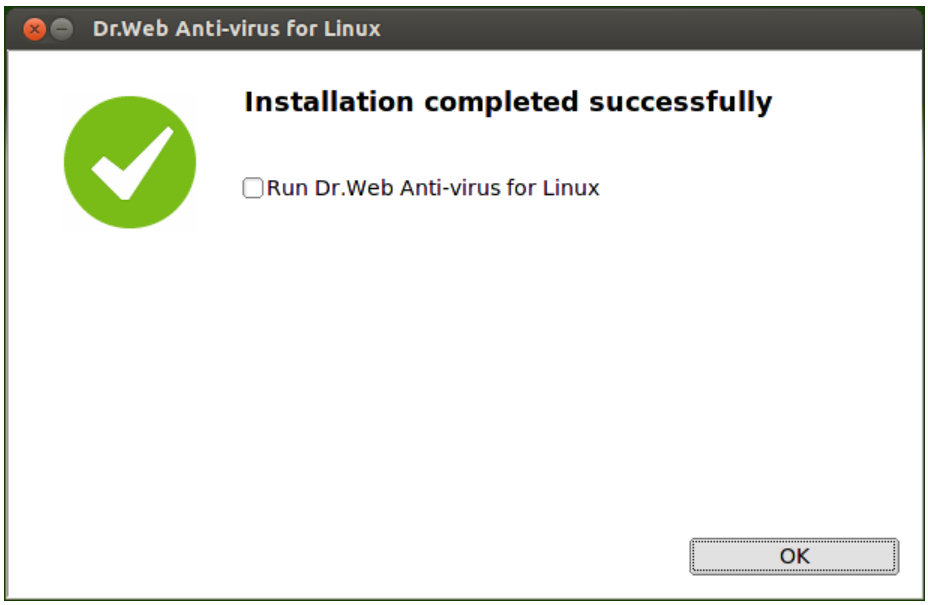


Picture 6. Installation progress bar



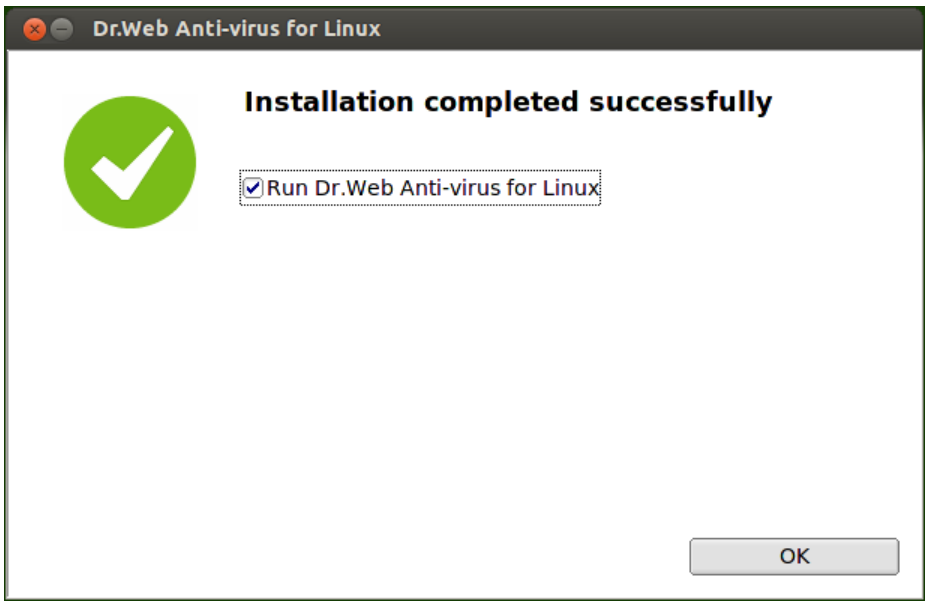
Picture 7. Viewing installation log file

4. After program files are successfully copied and all required adjustments to system files are made, the final page with the installation results displays.



Picture 8. Installation results page

5. To exit the Installation Wizard, click **OK.** If you want to open the **Dr.Web Anti-virus for Linux** in graphics mode once the installation completes, select the **Run Dr.Web Anti-virus for Linux** checkbox.



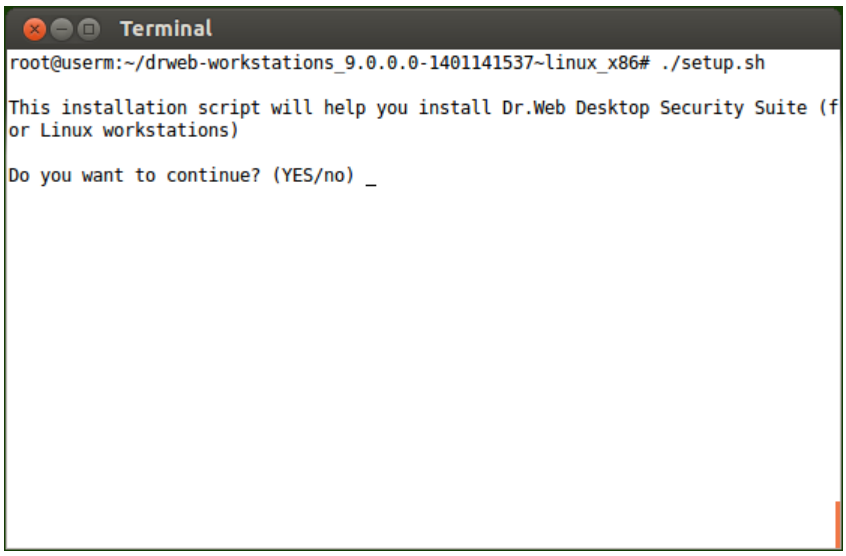
Picture 9. Selected option to start Anti-virus

If the installation process fails due to an error, the final page of the Installation Wizard will contain the corresponding message. In this case, exit the Installation Wizard, remove the problems that caused this error and start an installation procedure again.

Installing from Command Line

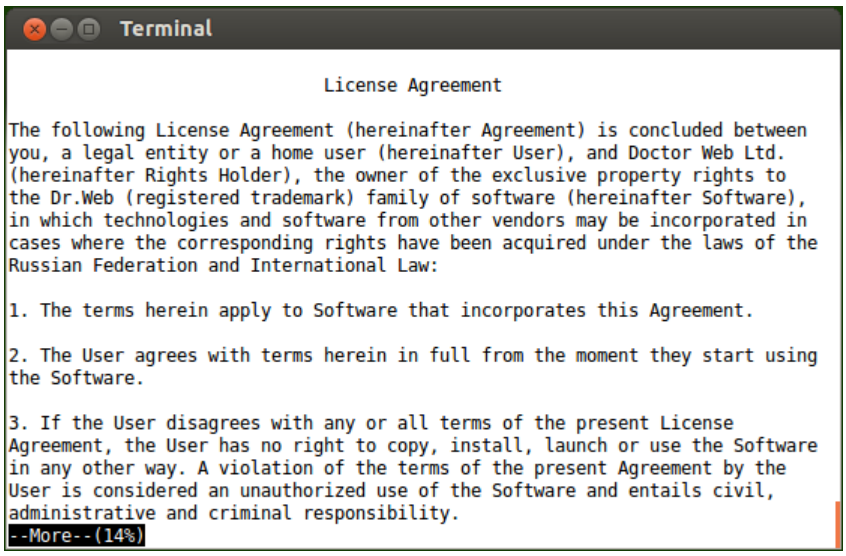
Once the installation program for the command line starts, the command prompt displays on the screen.

1. To start installation enter **`Yes`** or **`Y`** in response to the "Do you want to continue?" question. To exit the installer, enter **`No`** or **`N`**. In this case, installation is canceled.


Terminal
root@userm:~/drweb-workstations_9.0.0.0-1401141537~linux_x86# ./setup.sh
This installation script will help you install Dr.Web Desktop Security Suite (f
or Linux workstations)
Do you want to continue? (YES/no) _

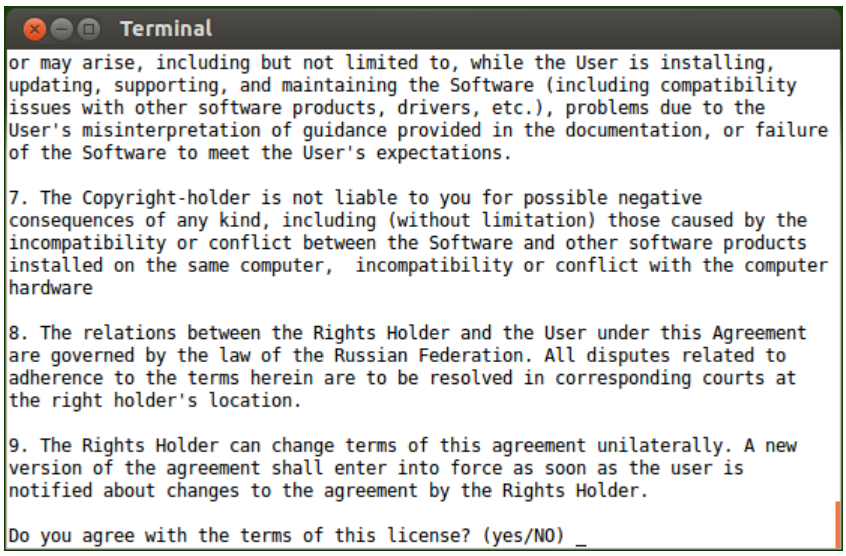
Picture 10. Command prompt to install the product

2. After that, you need to view the terms of the **Doctor Web** **License agreement** which displays on the screen. Press ENTER to line down or SPACEBAR to page down the text. Note that options to line up or page up the **License agreement** text are not provided.


Terminal
License Agreement
The following License Agreement (hereinafter Agreement) is concluded between
you, a legal entity or a home user (hereinafter User), and Doctor Web Ltd.
(hereinafter Rights Holder), the owner of the exclusive property rights to
the Dr.Web (registered trademark) family of software (hereinafter Software),
in which technologies and software from other vendors may be incorporated in
cases where the corresponding rights have been acquired under the laws of the
Russian Federation and International Law:
1. The terms herein apply to Software that incorporates this Agreement.
2. The User agrees with terms herein in full from the moment they start using
the Software.
3. If the User disagrees with any or all terms of the present License
Agreement, the User has no right to copy, install, launch or use the Software
in any other way. A violation of the terms of the present Agreement by the
User is considered an unauthorized use of the Software and entails civil,
administrative and criminal responsibility.
--More--(14%)

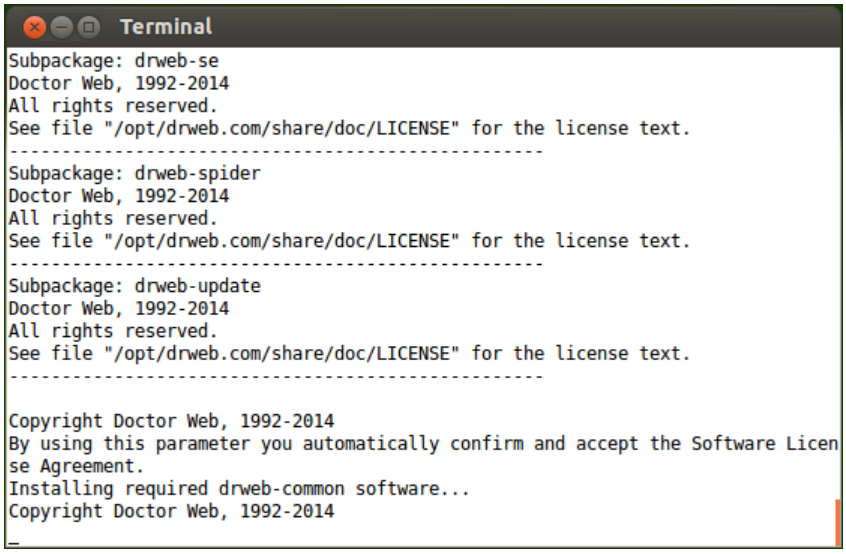
Picture 11. Viewing License Agreement text

3. After you read the **License agreement** text, you are prompted to accept the terms. Enter **`Yes`** or **`Y`** if you accept the **License agreement**. If you refuse to accept them, enter **`No`** or **`N`**. In the latter case, the installer exits.


Terminal
or may arise, including but not limited to, while the User is installing, updating, supporting, and maintaining the Software (including compatibility issues with other software products, drivers, etc.), problems due to the User's misinterpretation of guidance provided in the documentation, or failure of the Software to meet the User's expectations.
7. The Copyright-holder is not liable to you for possible negative consequences of any kind, including (without limitation) those caused by the incompatibility or conflict between the Software and other software products installed on the same computer, incompatibility or conflict with the computer hardware
8. The relations between the Rights Holder and the User under this Agreement are governed by the law of the Russian Federation. All disputes related to adherence to the terms herein are to be resolved in corresponding courts at the right holder's location.
9. The Rights Holder can change terms of this agreement unilaterally. A new version of the agreement shall enter into force as soon as the user is notified about changes to the agreement by the Rights Holder.
Do you agree with the terms of this license? (yes/NO) _

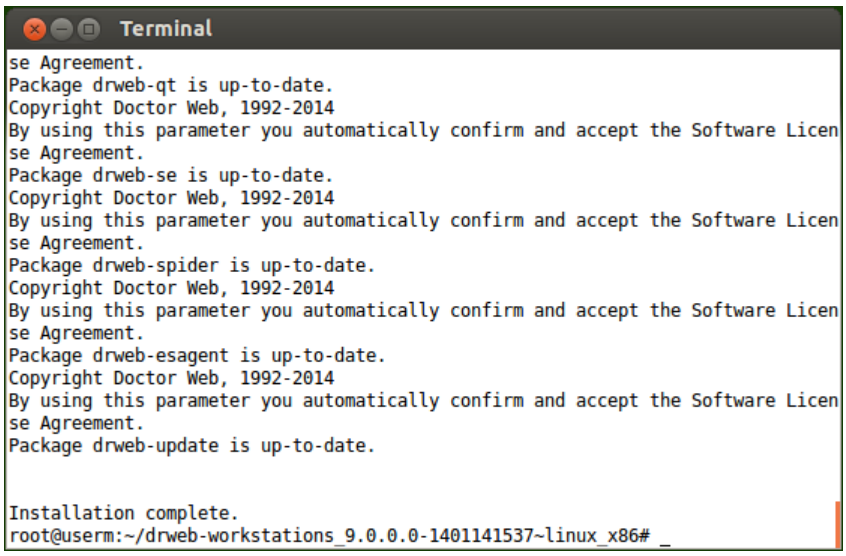
Picture 12. Accepting the License Agreement terms

4. After you accept the terms of the **License Agreement**, installation automatically starts. During the procedure, the information about the installation process, including the list of installed components, will be displayed on the screen.


Terminal
Subpackage: drweb-se
Doctor Web, 1992-2014
All rights reserved.
See file "/opt/drweb.com/share/doc/LICENSE" for the license text.
Subpackage: drweb-spider
Doctor Web, 1992-2014
All rights reserved.
See file "/opt/drweb.com/share/doc/LICENSE" for the license text.
Subpackage: drweb-update
Doctor Web, 1992-2014
All rights reserved.
See file "/opt/drweb.com/share/doc/LICENSE" for the license text.
Copyright Doctor Web, 1992-2014
By using this parameter you automatically confirm and accept the Software License Agreement.
Installing required drweb-common software...
Copyright Doctor Web, 1992-2014
_

Picture 13. Installation log

5. After the installation completes successfully, the corresponding message displays on the screen and the installer exits. If an error occurs, a message describing the error displays and the installer exits.


Terminal
se Agreement.
Package drweb-qt is up-to-date.
Copyright Doctor Web, 1992-2014
By using this parameter you automatically confirm and accept the Software Licen
se Agreement.
Package drweb-se is up-to-date.
Copyright Doctor Web, 1992-2014
By using this parameter you automatically confirm and accept the Software Licen
se Agreement.
Package drweb-spider is up-to-date.
Copyright Doctor Web, 1992-2014
By using this parameter you automatically confirm and accept the Software Licen
se Agreement.
Package drweb-esagent is up-to-date.
Copyright Doctor Web, 1992-2014
By using this parameter you automatically confirm and accept the Software Licen
se Agreement.
Package drweb-update is up-to-date.
Installation complete.
root@userm:~/drweb-workstations_9.0.0.0-1401141537~linux_x86# _

Picture 14. Installation complete message

6. To start working with the installed **Anti-virus**, run the product in one of the available ways.

If the installation process fails due to an error, remove the problems that caused this error and start an installation procedure again.

Installing from Dr.Web Repository

Dr.Web Anti-virus for Linux native packages are stored in the official **Dr.Web** repository at http://repo.drweb.com/drweb/. After you add the **Dr.Web** repository to the list of those used by your operating system package manager, you can install the product from native packages as you install any other programs from the operating system repositories. Required dependencies are automatically resolved.

All commands, mentioned below, for connecting repositories, import of digital signature keys, installation and removal of packages must be performed with administrative (`root`) privileges. To elevate the privileges, use the **`su`** command (change the current user) or the **`sudo`** command (execute the specified command with other user privileges).

Debian, Ubuntu (apt)

The repository for these operating systems is digitally signed. To enable correct operation, import a digital signature key using the following command:

```
wget -O - http://repo.drweb.com/drweb/drweb.key | apt-key add -
```

or

```
curl http://repo.drweb.com/drweb/drweb.key | apt-key add -
```

To connect the repository, add the following line to the `/etc/apt/sources.list` file:

```
deb http://repo.drweb.com/drweb/debian 9.0.0 non-free
```

Besides that, you can obtain the key automatically and connect to the repository of version 9.0.0 via downloading and installing of a special DEB packet. Link for downloading of the packet: http://repo.drweb.com/drweb-repo9.deb.

To install **Dr.Web Anti-virus for Linux** from the repository, use the following commands:

```
apt-get update
apt-get install drweb-workstations
```

You can also use alternative package managers (for example, **Synaptic** or **aptitude**) to install the product. Moreover, it is recommended to use alternative managers, such as **aptitude**, to solve a package conflict if it occurs.

Red Hat Enterprise Linux, Fedora, CentOS (yum)

Add the file with the content mentioned below to the `/etc/yum.repos.d` directory:

For 32-bit version

```
[drweb]
name=DrWeb - 9.0.0
baseurl=http://repo.drweb.com/drweb/el5/9.0.0/i386/
gpgcheck=1
enabled=1
gpgkey=http://repo.drweb.com/drweb/drweb.key
```

For 64-bit version

```
[drweb]
name=DrWeb - 9.0.0
baseurl=http://repo.drweb.com/drweb/el5/9.0.0/x86_64/
gpgcheck=1
enabled=1
gpgkey=http://repo.drweb.com/drweb/drweb.key
```

Besides that, you can connect to the repository of version 9.0.0 via downloading and installing of a special RPM packet. Link for downloading of the packet: http://repo.drweb.com/drweb-repo9.rpm.

To install **Dr.Web Anti-virus for Linux** from the repository, use the following command:

```
yum install drweb-workstations
```

You can also use alternative package managers (for example, **PackageKit** or **Yumex**) to install the product.

Adjusting SELinux Policies

If the used **Linux** distribution features **SELinux** (`Security-Enhanced Linux`), it is required to configure **SELinux** security policies to enable correct component operation (for example, operation of the scanning engine).

Moreover, installation from the installation file (`.run`) can fail if **SELinux** is enabled because an attempt to create the `drweb` user, under which **Dr.Web Anti-virus for Linux** components operate, can be blocked.

Before installing the product, check the **SELinux** operation mode with the **`getenforce`** command. The command outputs one of the following:

- **`Permissive`** – protection is active but a permissive strategy is used: actions that violate the security policy are not denied but information on the actions is logged.

- **Enforced** – protection is active and restrictive strategy is used: actions that violate security policies are blocked and information on the actions is logged.
- **Disabled** – **SELinux** is installed but not active.

If **SELinux** is operating in Enforced mode, it requires temporarily (while the product is installed and security policies are configured), change the mode to Permissive. For that purpose, use the **setenforce 0** command which temporarily (until the next reboot) enables Permissive mode for **SELinux**. To enable Enforced mode for **SELinux** again, use the **setenforce 1** command.

Note that regardless of the operation mode enabled with the **setenforce** command, restart of the operating system returns **SELinux** operation to the mode specified in the **SELinux** settings (file with **SELinux** settings usually resides in the /etc/selinux directory).

In general, when **audit** daemon is used on the system, the audit log file is /var/log/audit/audit.log. Otherwise, messages on blocked operations are saved to the general log file /var/log/messages.

To enable correct operation of the **Anti-virus** components when **SELinux** is active, it is required to compile special security policies once product installation completes.

Note that certain **Linux** distributions do not feature the utilities mentioned below. If so, you may need to install additional packages with the utilities.

To create required policies

1. Create a new file with the **SELinux** policy source code (.te file). This file defines restrictions applied to the module. The policy source code can be specified in one of the following ways:

   1) **Using** the **audit2allow** utility, which is the simplest method. The utility generates permissive rules from messages on access denial in system log files. You can set to search messages automatically or specify a path to the log file manually.

   The **audit2allow** utility resides in the policycoreutils-python or policycoreutils-devel package (for **RedHat Enterprise Linux, CentOS, Fedora** operating systems depending on the version) or in the python-sepolgen package (for **Debian, Ubuntu** OS).

   Please note that for **Fedora** version 19 it is required to install additionally the checkmodule package, otherwise the **audit2allow** utility returns an error.

   Example usage:

   ```
   # audit2allow -M drweb -i /var/log/audit/audit.log
   ```

   or

   ```
   # cat /var/log/audit/audit.log | audit2allow -M drweb
   ```

   In the given example, the **audit2allow** utility searches for messages on access denial in the audit.log file.

   ```
   # audit2allow -a -M drweb
   ```

   In the given example, the **audit2allow** utility automatically searches for messages on access denial.

   In both cases, the following two files are created: policy source file drweb.te and the drweb.pp policy module ready to install.

   In most cases, you do not need to modify the policy file created by the utility. Thus, it is recommended to go to step 4 for installation of the drweb.pp policy module. Note that the

audit2allow utility outputs invocation of the **semodule** command. By copying the output to the command line and executing it, you complete step 4. Go to step 2 only if you want to modify security policies which were automatically generated for **Dr.Web Anti-virus for Linux** components.

2) **Using** the **policygentool** utility. For that purpose, specify name of the module operation with which you want to configure and the full path to the executable file.

Note that the **policygentool** utility, included in the `selinux-policy` package for **RedHat Enterprise Linux** and **CentOS Linux** OS, may not function correctly. If so, use the **audit2allow** utility.

Example of policy creation via policygentool:

- for **drweb-se** (used by the anti-virus engine):

```
# policygentool drweb-se /opt/drweb.com/bin/drweb-se.real
```

- for **drweb-filecheck** (used by **Scanner**):

```
# policygentool drweb-filecheck /opt/drweb.com/bin/drweb-filecheck.real
```

You will be prompted to specify several common domain characteristics. After that, three files that determine the policy are created for each of the modules:

`[module_name].te`, `[module_name].fc` and `[module_name].if`.

2. If required, edit the generated policy source file `[module_name].te` and then use the **checkmodule** utility to create a binary mapping of the local policy source file (`.mod` file).

Note that to ensure success of the command, the `checkpolicy` package must be installed in the system.

Example usage

```
# checkmodule -M -m -o drweb.mod drweb.te
```

3. Create an installed policy module (`.pp` file) with the use of the **semodule_package** utility.

Example

```
# semodule_package -o drweb.pp -m drweb.mod
```

4. To install the created policy module, use the **semodule** utility.

Example

```
# semodule -i drweb.pp
```

After the system is restarted, **SELinux** is configured to allow correct operation of **Dr.Web Anti-virus for Linux**.

For details on **SELinux** operation and configuration, refer to documentation for the used **Linux** distribution.

Product Files Location

After installation of **Dr.Web Anti-virus for Linux**, its files reside in the `/opt`, `/etc`, and `/var` directories of the file system.

Structure of the used directories is as follows:

Directory	Content
/opt/drweb.com/	Executable files of product components and basic libraries required for operation of **Anti-virus**
/etc/opt/drweb.com	Files with component settings (by default) and license key file required for operation of **Anti-virus** in Standalone mode
/var/opt/drweb.com	Virus databases, **Dr.Web Virus-Finding Engine**, temporary files, and additional libraries required for **Anti-virus** operation.

Removing Dr.Web Anti-virus for Linux

Depending on the method of **Dr.Web Anti-virus for Linux** installation, you can remove the suite in one of the following ways:

1. Starting the uninstall program to remove the universal package distribution (for graphics or command-line mode, depending on the environment).
2. Deleting packages installed from the **Doctor Web** repository via the package system manager.

Removing Universal Package

You can remove **Dr.Web Anti-virus for Linux** installed from the distribution with the universal package for UNIX systems via the application menu of the desktop environment, or via the command line.

Removing program via application menu

On the application menu, click the **Dr.Web** item and select **Remove Dr.Web components**. Removal Wizard for graphics mode will start.

Removing program via command line

To remove **Anti-virus**, run the **remove.sh** script, which resides in the /opt/drweb.com/bin directory, using the following command:

```
# /opt/drweb.com/bin/remove.sh
```

Then an uninstall program starts (either in graphics or command-line mode, depending on the environment).

To start the uninstall program directly from the command line, use the following command:

```
# /opt/drweb.com/bin/uninst.sh
```

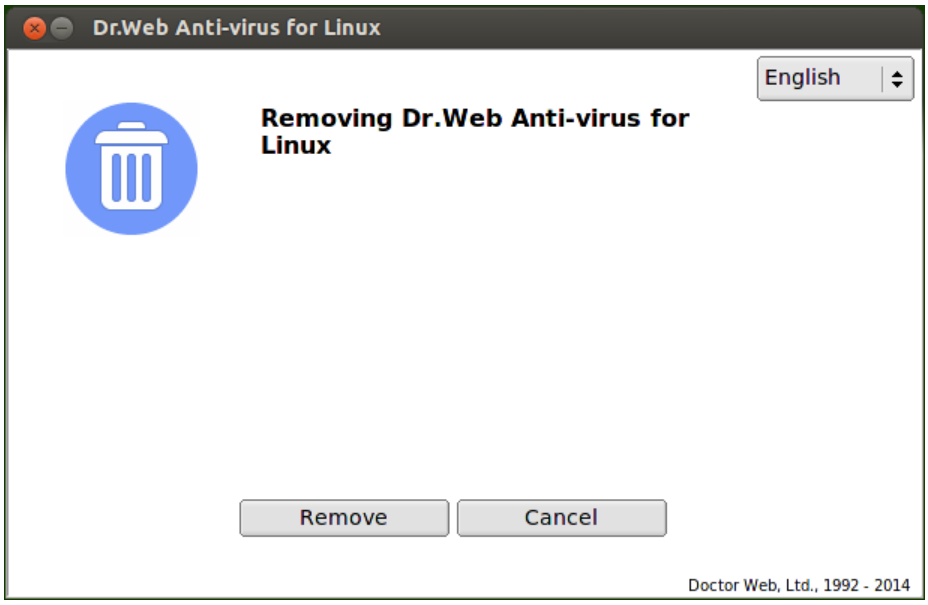
Removal of **Anti-virus** is described in the following chapters:

- Removing in Graphics Mode;
- Removing from Command Line.

Removing in Graphics Mode

Once the Removal wizard starts in graphics mode, its welcome page where you can select the language

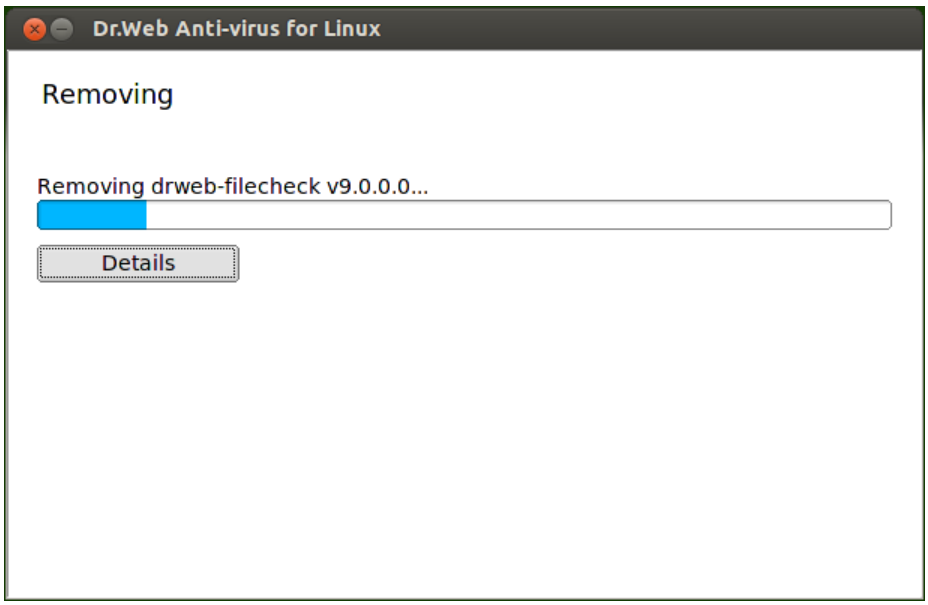
in the drop-down list in the upper-right corner.



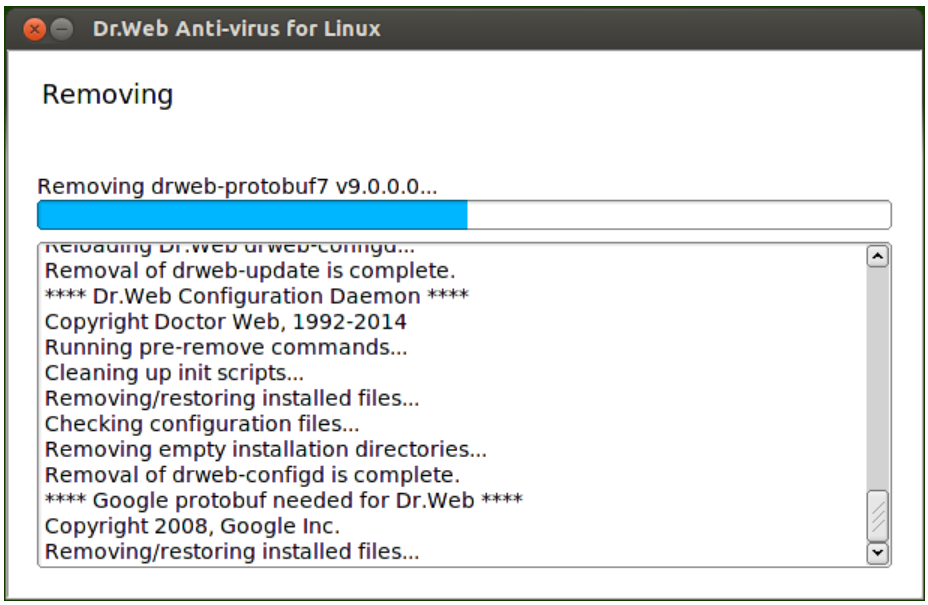
Picture 15. Welcome page

To uninstall **Dr.Web Anti-virus for Linux**, click **Remove**. To close the Removal Wizard, click **Cancel**.

After the removal starts, a page with the progress bar opens. If necessary, you can click the **Details** button and view the log.

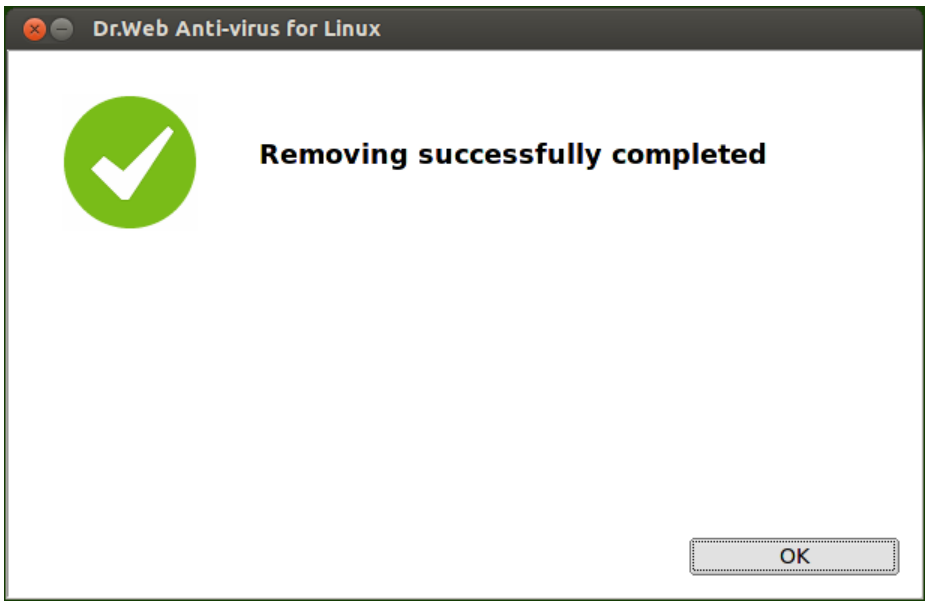


Picture 16. Removal progress bar



Picture 17. Viewing the log

After **Dr.Web Anti-virus for Linux** files are successfully removed and all necessary changes are made to the system files, a final page of the Removal Wizard displays notifying on successful operation results.



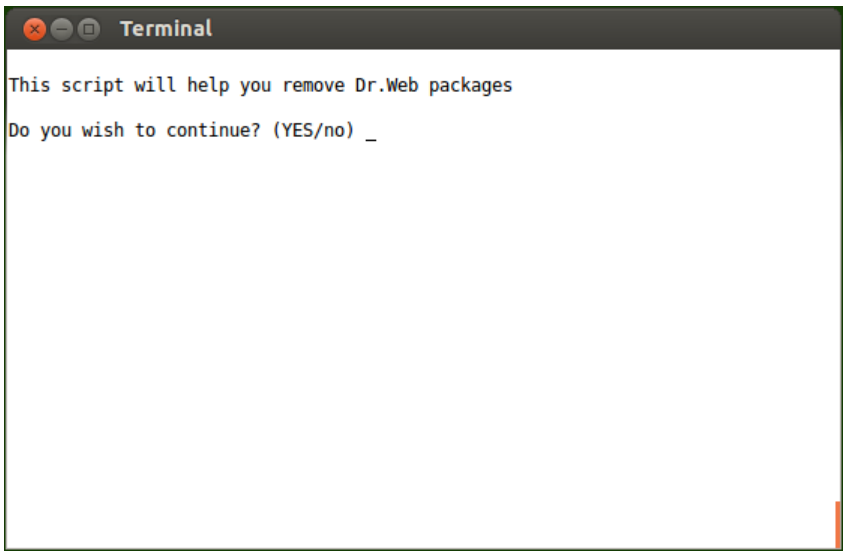
Picture 18. Removal Wizard results page

To close the Removal Wizard, click **OK**.

Removing from Command Line

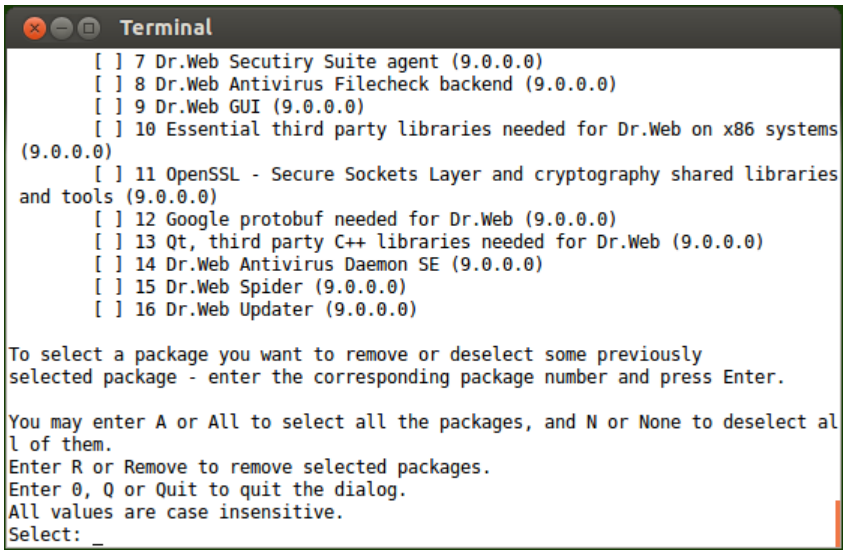
Once the removal program for command-line mode starts, the command prompt displays on the screen.

1. To start removal, enter **Yes** or **Y** in response to the "Do you wish to continue?" question. To exit the removal program, enter **No** or **N**. In this case, removal will be canceled.



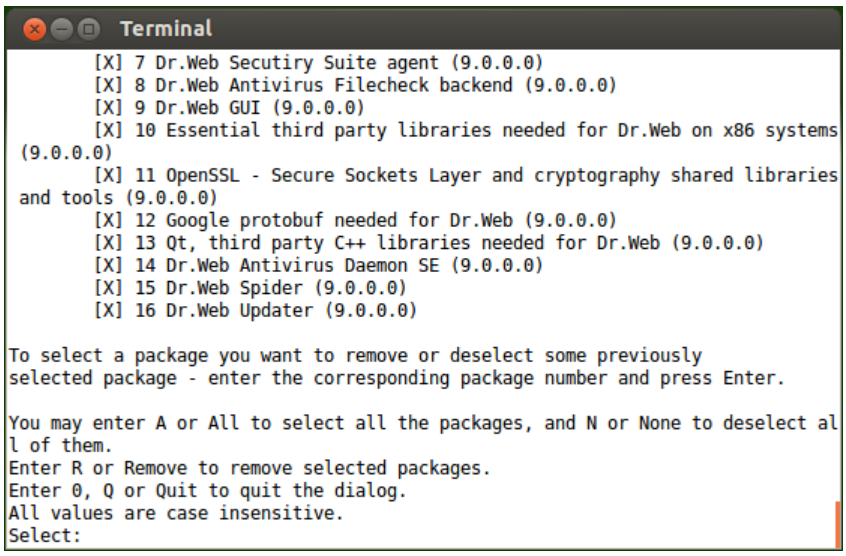
Picture 19. Command prompt to uninstall the product

2. After that, a list of installed **Dr.Web Anti-virus for Linux** components is output.


Terminal
[ ] 7 Dr.Web Secutiry Suite agent (9.0.0.0)
[ ] 8 Dr.Web Antivirus Filecheck backend (9.0.0.0)
[ ] 9 Dr.Web GUI (9.0.0.0)
[ ] 10 Essential third party libraries needed for Dr.Web on x86 systems (9.0.0.0)
[ ] 11 OpenSSL - Secure Sockets Layer and cryptography shared libraries and tools (9.0.0.0)
[ ] 12 Google protobuf needed for Dr.Web (9.0.0.0)
[ ] 13 Qt, third party C++ libraries needed for Dr.Web (9.0.0.0)
[ ] 14 Dr.Web Antivirus Daemon SE (9.0.0.0)
[ ] 15 Dr.Web Spider (9.0.0.0)
[ ] 16 Dr.Web Updater (9.0.0.0)
To select a package you want to remove or deselect some previously selected package - enter the corresponding package number and press Enter.
You may enter A or All to select all the packages, and N or None to deselect all of them.
Enter R or Remove to remove selected packages.
Enter 0, Q or Quit to quit the dialog.
All values are case insensitive.
Select: _

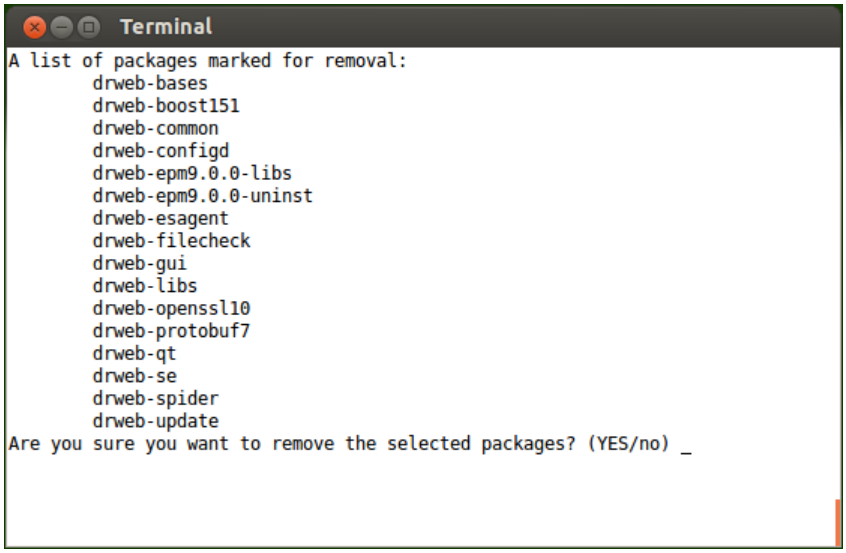
Picture 20. Viewing the list of installed components

3. To continue the removal, select the components to be deleted. For selecting a certain component, enter its number in the list. Note that all packages depending on a selected package are also automatically selected for removal.
   - To select all listed components, enter **`All`** or **`A`** instead of a component number
   - To reject selection of the packages, enter **`None`** or **`N`** instead of a component number.
   - To cancel removal, enter **`0`**, **`Q`** or **`Quit`** instead of a component number. If so, the removal program exits.


Terminal
[X] 7 Dr.Web Secutiry Suite agent (9.0.0.0)
[X] 8 Dr.Web Antivirus Filecheck backend (9.0.0.0)
[X] 9 Dr.Web GUI (9.0.0.0)
[X] 10 Essential third party libraries needed for Dr.Web on x86 systems (9.0.0.0)
[X] 11 OpenSSL - Secure Sockets Layer and cryptography shared libraries and tools (9.0.0.0)
[X] 12 Google protobuf needed for Dr.Web (9.0.0.0)
[X] 13 Qt, third party C++ libraries needed for Dr.Web (9.0.0.0)
[X] 14 Dr.Web Antivirus Daemon SE (9.0.0.0)
[X] 15 Dr.Web Spider (9.0.0.0)
[X] 16 Dr.Web Updater (9.0.0.0)
To select a package you want to remove or deselect some previously selected package - enter the corresponding package number and press Enter.
You may enter A or All to select all the packages, and N or None to deselect all of them.
Enter R or Remove to remove selected packages.
Enter 0, Q or Quit to quit the dialog.
All values are case insensitive.
Select:

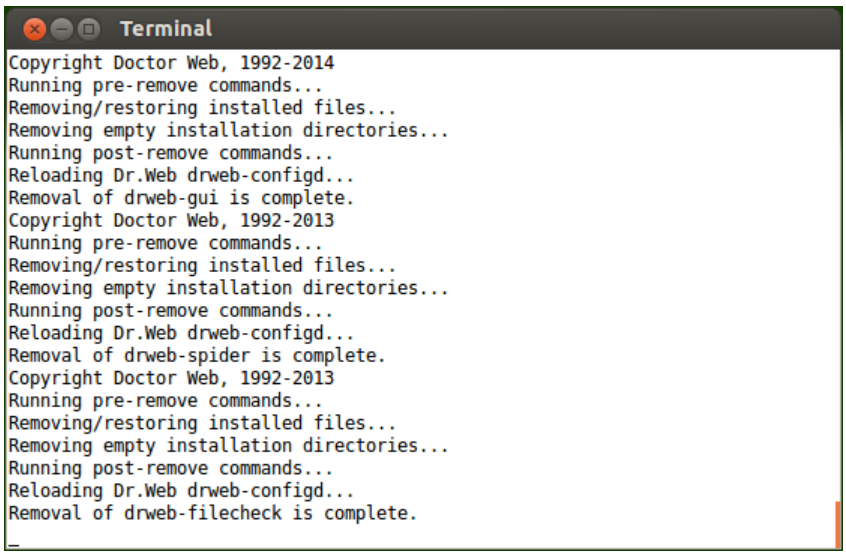
Picture 21. Selection of components to be removed

4. After you select the components to be removed, enter **Remove** or **R** to start the process.



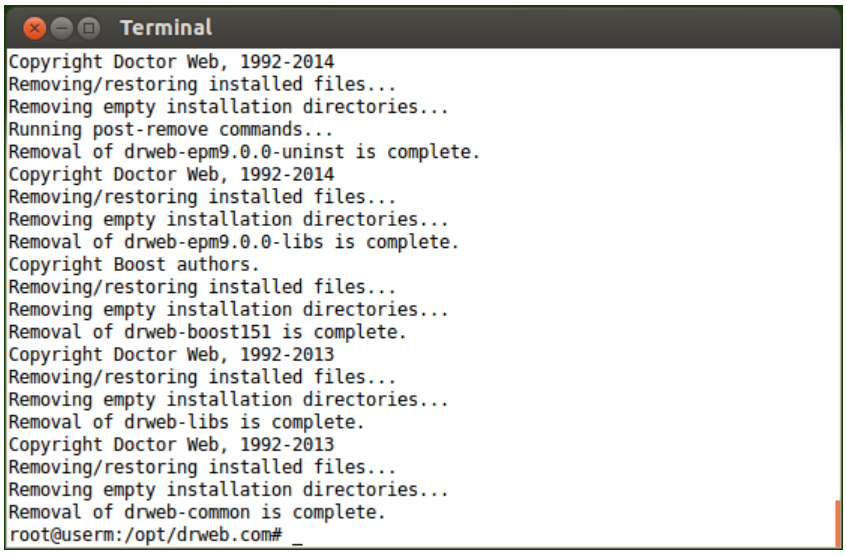
Picture 22. Component removal confirmation

5. On the next page, view the list of packages selected for removal and confirm the action by entering **Yes** or **Y**. If you choose not to delete the components, exit the removal program by entering **No** or **N**.



Picture 23. Uninstallation log

6. After removal of the selected components starts, messages about the removal process are output in the screen and logged.



Picture 24. Uninstallation complete message

7. Once the removal completes, the program outputs the corresponding message and exits.

Removing Product Installed from Repository

All commands mentioned below for package removal require administrative (`root`) privileges. To elevate the privileges, use the **`su`** command (change the current user) or the **`sudo`** command (execute the specified command with other user privileges).

Debian, Ubuntu (apt)

To remove **Dr.Web Anti-virus for Linux**, enter the following command:

```
apt-get remove drweb-workstations
```

To remove all installed **Dr.Web** packages, enter the following command (in certain operating systems, a '*' character must be escaped: '*'):

```
apt-get remove drweb*
```

To automatically remove all packages that are no longer used, enter the following command:

```
apt-get autoremove
```

Note special aspects of removal with the **apt-get** command:

1. The first mentioned version of the command removes only the `drweb-workstations` package; all other packages that could be automatically installed to resolve dependencies remain in the system.
2. The second mentioned version of the command removes all packages which name starts with "`drweb`" (standard name prefix for **Dr.Web** products). Note that this command removes all packages with this prefix, not only those of **Dr.Web Anti-virus for Linux**.
3. The third mentioned version of the command removes all packages that were automatically installed to resolve dependencies of other packages and are no longer necessary (e.g., due to their removal). Note that this command removes all packages that are not used, not only those of **Dr.Web Anti-virus for Linux**.

You can also use alternative package managers (for example, **Synaptic** or **aptitude**) to remove packages.

Red Hat Enterprise Linux, Fedora, CentOS (yum)

To remove **Dr.Web Anti-virus for Linux**, enter the following command:

```
yum remove drweb-workstations
```

To remove all installed **Dr.Web** packages, enter the following command (in certain operating systems, a '*' character must be escaped: '*'):

```
yum remove drweb*
```

Note special aspects of removal with the **yum** command:

1. The first mentioned version of the command removes only the `drweb-workstations` package; all other packages that could be automatically installed to resolve dependencies remain in the system.
2. The second mentioned version of the command removes all packages which name starts with "`drweb`" (standard name prefix for **Dr.Web** products). Note that this command removes all packages with this prefix, not only those of **Dr.Web Anti-virus for Linux**.

You can also use alternative package managers (for example, **PackageKit** or **Yumex**) to remove packages.

Working with Dr.Web Anti-virus for Linux

You can work with **Dr.Web Anti-virus for Linux**

- via the graphical interface (in graphic desktop environment)
- from the command line of the operating system, including terminal emulators for graphics mode.

To start **Anti-virus** in graphics mode, select the **Dr.Web for Linux** item in the application menu or enter the following command in the operating system command line

```
$ drweb-gui
```

In this case, if the desktop environment is available, **Dr.Web Anti-virus for Linux** is started in graphics mode.

For details on managing the **Anti-virus** operation, refer to the Operation from the command line section.

Under normal operation of **Dr.Web Anti-virus for Linux**, all its components are run automatically (some of them are run on operating system startup, others – at request of other components) and do not require manual intervention.

Regardless of the selected way to install **Dr.Web Anti-virus for Linux**, after the installation completes, you need either to activate the license, or install the key file if already obtained, or connect **Anti-virus** to the central protection server (see License Management).

Until you do that, **anti-virus protection is disabled.**

Operating in Graphics Mode

Dr.Web Anti-virus for Linux graphical interface is a windowed application functioning in the graphical desktop environment and used for management of **Anti-virus** operation.

Main functions

The graphical interface of **Dr.Web Anti-virus for Linux** allows to

1. View status of **Dr.Web Anti-virus for Linux** operation, including status of virus databases and period of license validity.
2. Start and stop **SpIDer Guard**.
3. Start file scanning on demand in one of the following modes:
   - **Express scan** to check system files and most critical system objects;
   - **Complete scan** to check all accessible files in the file system;
   - **Custom scan** to check only those files and directories that are specified by the user, or special objects (disk boot sectors, active processes)

   You can specify files to be scanned either by selecting files and directories before scanning starts or by dragging and dropping them from the file manager window to the Main page (see below) or Scan page of the **Anti-virus** window.
4. View all threats detected on the computer by **Dr.Web Anti-virus for Linux** during current operation in graphics mode, including neutralized and skipped threats and quarantined objects.
5. View objects moved to **Quarantine**, delete, or restore them.
6. Configure parameters of **Dr.Web Anti-virus for Linux** operation including:
   - Actions to be automatically applied to detected threats (depending on their type) by **Scanner**

and **SpIDer Guard**;

- List of files and directories that should not be scanned by **Scanner** or checked by **SpIDer Guard**;
- Schedule of scanning tasks including the period and type of performed scanning, and list of objects that are to be scanned;
- Operation mode (status of connection to the central protection server).

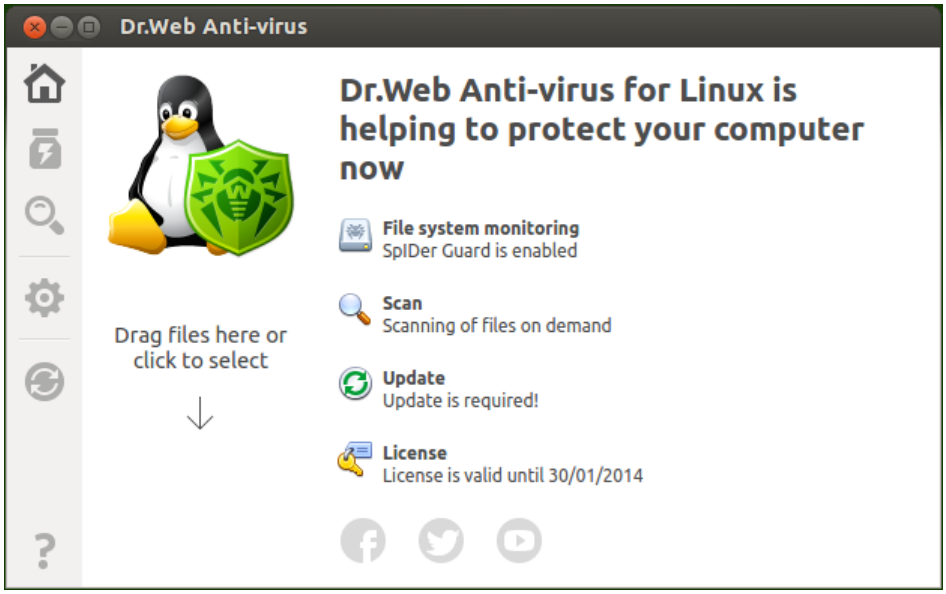
8. License management (performed via **License Manager**).

To enable correct operation, ensure that all service components are running before **Anti-virus** is started; otherwise, it shuts down immediately after the startup having displayed the corresponding warning message.

Under normal operation, all necessary components are started automatically and do not require user intervention.

Appearance

The appearance of the **Anti-virus** Main page is presented in the picture below.



Picture 25. Main window of the Dr.Web Anti-virus for Linux

The left pane of the window displays navigation buttons which allow to perform the following actions.

Button	Description
Continuously enabled	
	Opens the Main page where you can • enable or disable **SpIDer Guard**; • start scanning of file system objects (files, boot records) and running processes; • view the virus database status and update them if necessary; • start **License Manager** to view the current license status and register a new license if necessary.
	Opens the **Quarantine** page where you can view quarantined files, delete them, or restore.
	Opens the page where you can start file scanning, select the scanning type and specify objects to be scanned, including currently running processes.

Button	Description
	Opens the page with **Anti-virus** settings including • **Scanner** settings; • **SpIDer Guard** settings; • Run scannings by a schedule. Moreover, on this page you can configure settings of Central protection mode.
	Provides access to **Doctor Web** reference materials and resources • Product information; • User manual; • Official forum; • Technical support; • Personal user's webpage **My Dr.Web.** All links open webpages in the browser installed in your system.
Visible depending on certain conditions	
	Opens the page with the list of incomplete scanning tasks. The button is visible on the pane only if at least one scanning task is in progress.
	Opens the page with results of complete scanning tasks. The button changes its colour depending on the scanning results 1) Green – all scanning tasks completed successfully; all detected threats, if any, are neutralized. 2) Red – some of the detected threats are not neutralized. 3) Yellow – at least one of the scanning tasks failed. The button is visible on the pane only if at least one scanning task was started.
	Opens the page where threats detected by **Scanner** or **SpIDer Guard** are listed. The button is visible on the pane only if at least one threat is detected.
	Opens the page with **SpIDer Guard** settings. The button is visible on the pane only if the page with **SpIDer Guard** settings was opened from the Main page.
	Opens the page with update settings. The button is visible on the pane only if the page with update settings was opened from the Main page.
	Opens the **License Manager** page. The button is visible only if the **License Manager** page was opened from the Main page.

Main Page

On the Main page you can find the target pane where you can drag and drop files and directories to be scanned. The pane is marked with the **Drag files here or click to select** label and an image of a down arrow. After objects are dragged and dropped from the file manager to the Main page, their scanning starts (if the **Scanner** is already scanning other objects, the new scanning task is queued).

On this page, the following buttons are available:

- **File system monitoring** – displays the current status of **SpIDer Guard**. Click this button to open the **SpIDer Guard** page with the component settings where you can start or stop **SpIDer Guard** as well as view statistics on its operation.
- **Scan** – allows to open the page where you can start scanning of files and other file system objects (for example, boot records).

- **Update** – displays the current status of virus databases. Click this button to open the page with update status where you can start an updating process, if required.
- **License** – displays status of the current license. Click this button to open the **License Manager** page where you can find more detailed information on the current license as well as purchase and register a new license if required.

Indicator in desktop tray

When **Anti-virus** is operating in graphics mode, a status indicator is available in the desktop tray. The indicator is used for displaying pop-up notifications and providing access to the application menu.

Starting and Shutting Down Graphical Interface

All **Dr.Web Anti-virus for Linux** components are automatically run by default (some of the components are run on operating system startup, others only by request from other components) and do not require user intervention in their operation.

Starting Anti-Virus in Graphics Mode

To start **Dr.Web Anti-virus for Linux** in graphics mode, select the **Dr.Web for Linux** item on the **Applications Menu.**

You can also start **Dr.Web Anti-virus for Linux** in graphics mode from the command line.

Shutting Down Anti-Virus

To shut down **Dr.Web Anti-virus for Linux**, close the window using the standard close button on the title bar.

Note that service components continue their operation after **Anti-virus** shuts down. The same is actual for **SpIDer Guard** as well, but the component cannot be accessed via the indicator in the system tray. Thus, it is not recommended to close the **Anti-virus** window when **SpIDer Guard** is enabled (minimize the window instead).

Under normal operation, operation of all necessary service components does not require user intervention.

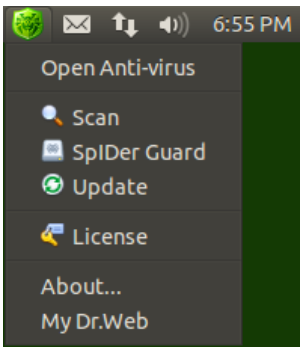
Indicator in desktop tray

When **Dr.Web Anti-virus for Linux** is operating in graphics mode (if supported by the used graphical environment), an indicator displays in the tray as the **Anti-virus** icon. The indicator is used for displaying the application status and providing access to the **Anti-virus** menu. If any problem occurs (e.g., the virus databases are outdated, license is about to expire), the indicator displays with an exclamation icon.

The indicator is used for displaying pop-up notifications that inform the user on important events of **Anti-virus** operation, such as:

- Detected threats (including those detected with **SpIDer Guard**);
- License validity period is about to expire.

Once the icon is clicked, the **Anti-virus** menu displays on the screen.



Picture 26. Dr.Web Anti-virus for Linux menu

When the **Open Anti-virus, Scan, SpIDer Guard,** or **License** item is selected, the **Anti-virus** window displays the corresponding page. When the **About...** item is selected, a page with brief information on the company, product name, and product version displays. When the **My Dr.Web** item is selected, the personal user page on the **Doctor Web** official website opens in the browser (a valid Internet connection is required).

If the indicator notifies on problems in **Anti-virus** operation, the menu item of the component which caused the problem is discolored to red (in the picture above, the indicator notifies on disabled **SpIDer Guard** and expired license validity period). So, you can solve the problem by opening the corresponding page of **Anti-virus** and performing required actions.

Note that after the **Anti-virus** window is closed, the indicator does not display in the tray and thus, **SpIDer Guard** cannot show notifications. Due to this, it is not recommended to close the **Anti-virus** window when **SpIDer Guard** is enabled (minimize the window instead).

In different desktop environments, appearance and behavior of the indicator can differ from the ones described above; for example, icons may not display in the drop-down menu.

Threat Detection and Neutralization

Search and neutralization of threats can be started either by **Scanner** on user demand, or as scheduled, or by **SpIDer Guard**.

- To enable or disable **SpIDer Guard**, open the page with its operation settings.
- To view current tasks of **Scanner** or manage them, open the page for task management.
- To view threats detected by **Scanner** or during **SpIDer Guard** checks, open the page with listed threats page.
- To manage quarantined threats, open the Quarantine view page.
- To configure **Dr.Web Anti-virus for Linux** reaction on detected threats, open the Settings page. On this page, you can also set schedule to start scanning.

Please note that in case if the **Anti-virus** is operating in Central protection mode and launching of scanning by user demand is prohibited on central protection server, the Scan page of the **Anti-virus** window will be disabled. Moreover, in this case the **Scanner** will not launch scannings even if they are scheduled.

Scanning on Demand

Scanning Types

On user demand, scanning in one of the following modes can be started:

- *Express scan* – scan of critical system objects that are at high risk to be compromised (boot records, system files, etc.).
- *Complete scan* – scan of all file system objects available for the user under whom **Anti-virus** is started.
- *Custom scan* – scan of file system objects or other special objects specified by the user.

If **Anti-virus** is operating in Central protection mode and launch of scanning at user request is prohibited on the Central protection server, this page is disabled.

Scanning can increase processor load, which can cause the battery to discharge faster. Thus, it is recommended to perform a scan of a portable computer when it is plugged in.

Starting Scanning

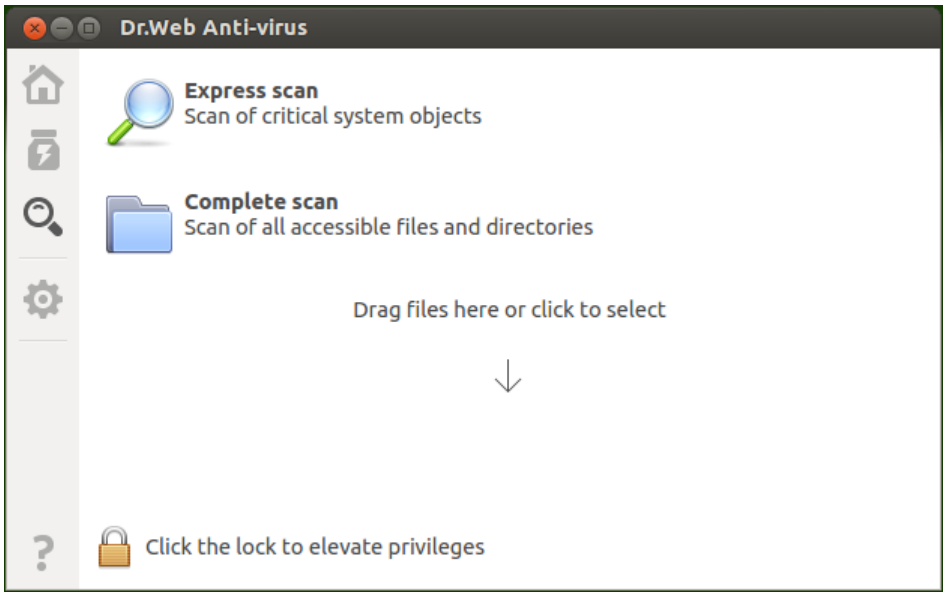
To start scanning

- Click the button on the navigation pane.

or

- Click the **Scan** button on the Main page.

The page with scan types opens. To start *Express* or *Complete* scan, click the corresponding button. Once one of these buttons is clicked, scanning process automatically starts.


Dr.Web Anti-virus
Express scan
Scan of critical system objects
Complete scan
Scan of all accessible files and directories
Drag files here or click to select
Click the lock to elevate privileges

Picture 27. Select scan type page

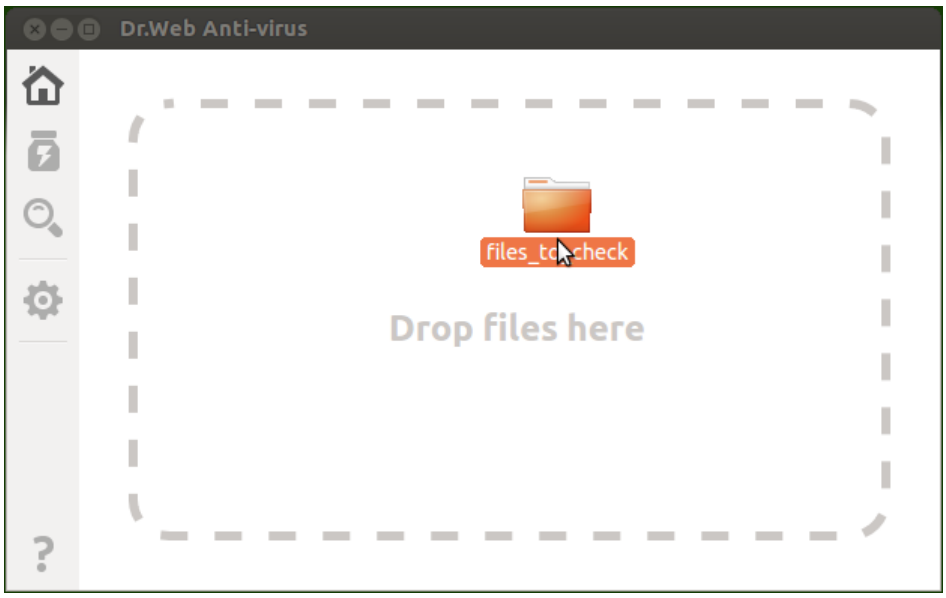
Scanning is performed with current application privileges. If the user whose privileges are currently active does not have superuser permissions, all files and directories that are not accessible to this user cannot be scanned. To enable check of all required files on which you do not have owner permissions, elevate the application privileges before scanning starts. For details, refer to the Managing Application Privileges section.

To start *Custom scan* of certain files and directories, do one of the following:

- **Drag and drop required objects**

  Drag and drop required files and directories from the system File Manager window to the area marked with a special label **Drag files here or click to select** and an image of a down arrow. You can also drag and drop the objects to the Main page.

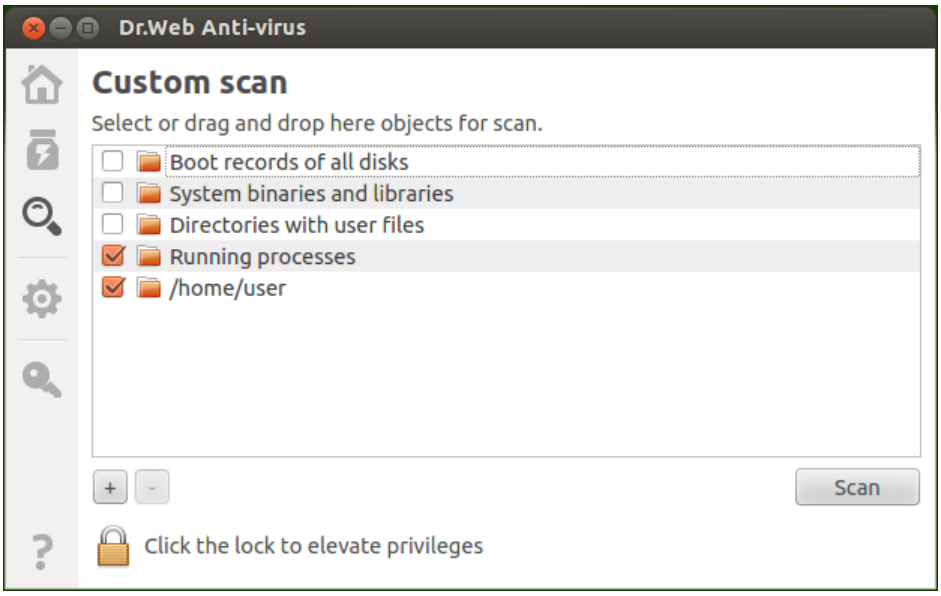
  When dragging objects over the page, it changes to the pane indicated with a dashed line and with the **Drop files here** label. To start scanning, drop the dragged objects onto the target area by releasing the mouse button.



Picture 28. Target area where objects are dropped for scanning

- **List the objects to be scanned.**

  To select the objects for scanning, click the target area. The window where you can select system objects for Custom scan opens.



Picture 29. List of objects for scanning

The list of objects for Custom scan contains four predefined items:

- *Boot records of all disks.* If you enable this item, all boot records of all available disks are selected for scanning.
- *System binaries and libraries.* If you enable this item, all directories with system binaries are selected for scanning (`/bin`, `/sbin`, etc.);
- *Directories with user files.* If you select this item, all directories where user files and files of the current session reside are selected for scanning (`/home/<username>` (`~`), `/tmp`, `/var/mail`, `/var/tmp`).
- *Running processes.* If you select this item, binary executable files containing code of currently running processes are selected for scanning. At that, if a threat is detected, not only the malicious object is neutralized but also the active process is terminated.

Editing the list of Custom scan objects

If required, you can add custom paths to the list of objects for scanning. For that purpose, drag and drop necessary objects (paths to the objects are automatically added to the list) or click the "+" button below the list. In this case, a standard dialog window opens, where you can select required objects (a file or a directory). After you select an object, click **Open.** To remove all selected paths from the list, click the "–" button.

Hidden files and directories are not displayed in the file chooser by default. To view such objects, right-click the list of files in the file chooser and select **Show hidden files.**

The first four items in the list are predetermined and cannot be removed even if the corresponding checkboxes are selected. Moreover, if at least one of the predetermined item is selected, the – button is unavailable.

Starting Custom scan of listed objects

To start Custom scan of listed objects, select all required files or directories and click **Scan.** Once the button is clicked, scan of the selected objects starts.

After scanning starts, the task is added to the queue which contains all scanning tasks of the current session: complete tasks, tasks in progress, and pending tasks. You can view the list of tasks and manage them on the scan task management page.

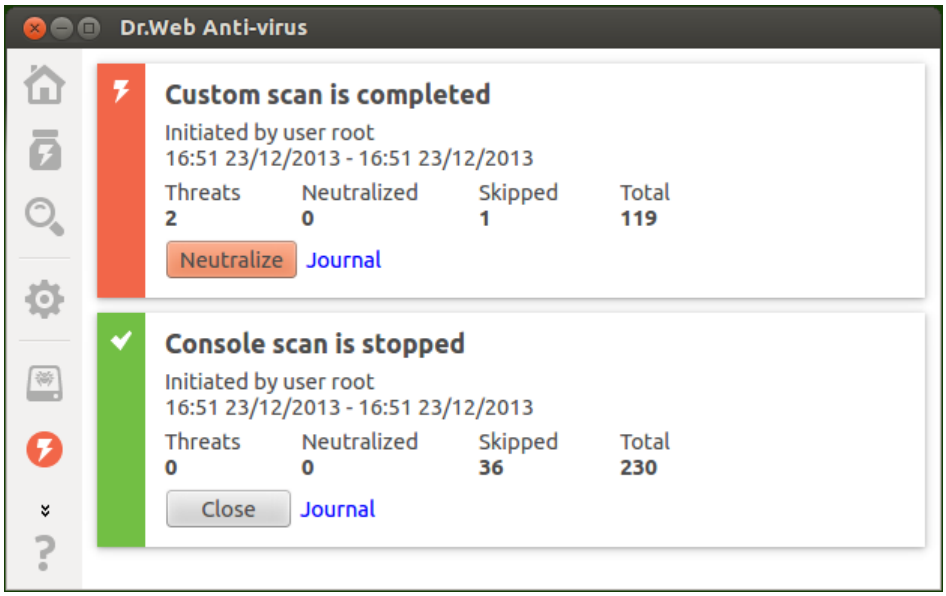
Managing Scan Tasks

You can view the list of created tasks and tasks in progress on the special **Dr.Web Anti-virus for Linux** page. If at least one task is queued, a button that opens the page with the task list becomes visible on the navigation pane. Depending on the status of the queued tasks, the button has one of the following icons:

	At least one of the tasks is not complete (icon is animated).
	All scanning tasks in the list are complete or stopped by the user; no threat is detected or all detected threats are successfully neutralized.
	All scanning tasks in the list are complete or stopped by the user; some of the detected threats are not neutralized.

All scanning tasks in the list are complete or stopped by the user. Some of the tasks failed.

Tasks are sorted by date (from the first created task to the most recent).



Picture 30. Task management page

For each listed task, the following information is available:

- Scan type (*Express scan*, *Complete scan*, *and Custom scan*, or other types of scanning; for details, see below);
- Name of the user who started scanning (if unknown, the system UID is displayed);
- Date of task creation and completion (if complete);
- Number of detected threats, neutralized threats, skipped files, and total number of scanned objects.

The status of the task is indicated with the colour mark assigned to the listed task. The following colours are used:

– Scanning is not complete or is pending.

– Scanning is complete or stopped by the user; no threat is detected or all detected threats are neutralized.

– Scanning is stopped due to an error.

– Scanning is complete or stopped by the user; at least one detected threat is not neutralized.

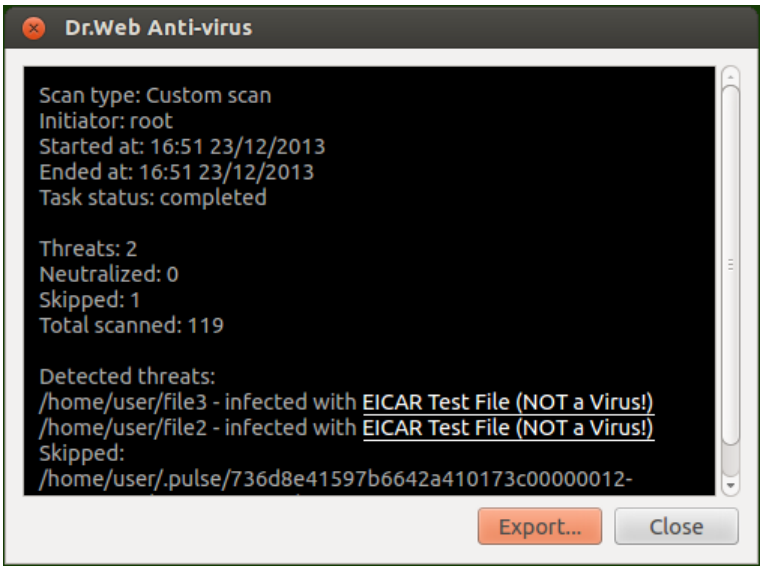
Note that the list contains scanning tasks performed by **Scanner** in the current session, not just the tasks created by the user in graphics mode. Other types of scanning can be the following:

- *Console scanning* – scanning initiated by the user or an external application via the command-line interface;
- *Centralized scanning* – scanning initiated by the central protection server;
- *Scheduled scanning* – scanning started automatically according to the specified schedule.

On the task description area, one of the following buttons is available:

- **Cancel** – cancel the pending scanning task. The button is available if the task is pending. Once the button is clicked, the task completes. Information on the task remains in the list.
- **Stop** – stop the scanning task which is in progress. After you click this button, the stopped task cannot be resumed. The button is available if the task is in progress. Information on the stopped task remains in the list.
- **Close** – close information on the complete task and delete the task from the list. The button is available if the task is not complete and if all detected threats are neutralized.
- **Neutralize** – neutralize threats. The button is available if the task is complete and some of the detected threats are not neutralized.
- **Details** – open the list with detected threats and neutralize them. The button is available if the task is complete and some of the detected threats are not neutralized.

Click **Journal** to display information on scanning results including detailed information on the task and the list of detected threats, if any.



Picture 31. Detailed information on scanning results

Note: File systems of UNIX-like OS, such as **Linux,** can contain special objects that appear as named files but are not actual files containing data (for example, such objects are symbolic links, sockets, named pipes, and device files). They are called *special* files as opposed to usual (*regular*) ones. **Anti-virus** always skips special files during scanning.

Click **Export...** to save information on scanning to the text file. Click the name of a detected threat to open a webpage with information on the threat in your browser (a threat name is a link to the official **Doctor Web** website; a valid Internet connection is required).

To any threat detected during scanning started in graphics mode (including a scheduled scanning), **Anti-virus** applies actions that are specified in the settings on the **Scanner** tab.

Note that threat neutralization settings specified on the **Scanner** tab are not used for *centralized* and *console* scanning.

To view all detected threats, open the page with listed detected threats.

Monitoring File System

SpIDer Guard is an anti-virus monitor which checks all created and modified file system objects.

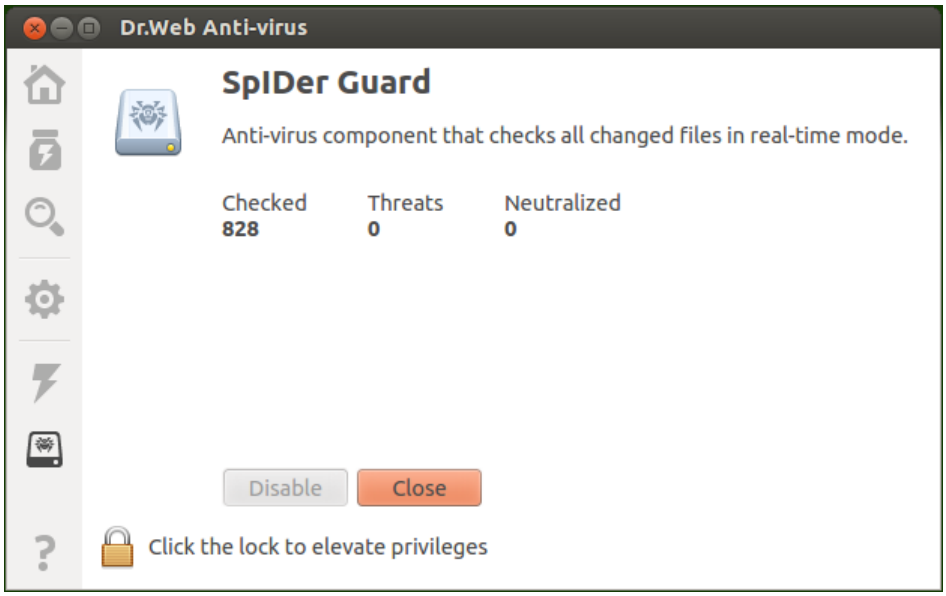
On the **Anti-virus** main window, you can manage **SpIDer Guard** operation

- start and stop file system monitoring
- view statistics on component operation and list of detected threats
- configure the following operation parameters:
  - reaction to detected threats
  - list of exclusions

Operation Management

You can start and stop **SpIDer Guard**, as well as view statistics on its operation on a special page.

To open the page, click **File system monitoring** on the Main page or click the button on the navigation pane (the button is visible only if the page with the monitor settings is opened from the Main page).



Picture 32. Page with SpIDer Guard settings

On the page with the monitor settings, the following information is available:

- Status of **SpIDer Guard** and information on startup errors (if any).
- Statistics on **SpIDer Guard** operation (number of checked objects, number of detected threats, number of neutralized threats).

To enable monitoring of the file system, click **Enable**. To disable monitoring, click **Disable.**

To disable file system monitoring, the application must have elevated privileges. For details, refer to Managing Application Privileges.

If **Anti-virus** is operating in Central protection mode, this option is enabled in dependence on permissions are specified on the server.

Status of the file system monitor **SpIDer Guard** (enabled or disabled) is indicated with one of the following colours:

– **SpIDer Guard** is enabled and is protecting the file system.

– **SpIDer Guard** is disabled and is not protecting the file system.

To close the **SpIDer Guard** settings page, click **Close**.

The list of threats detected by **SpIDer Guard** in the current session of the **Dr.Web Anti-virus for Linux** GUI displays on the page with listed threats (the page is available only if at least one threat is detected).

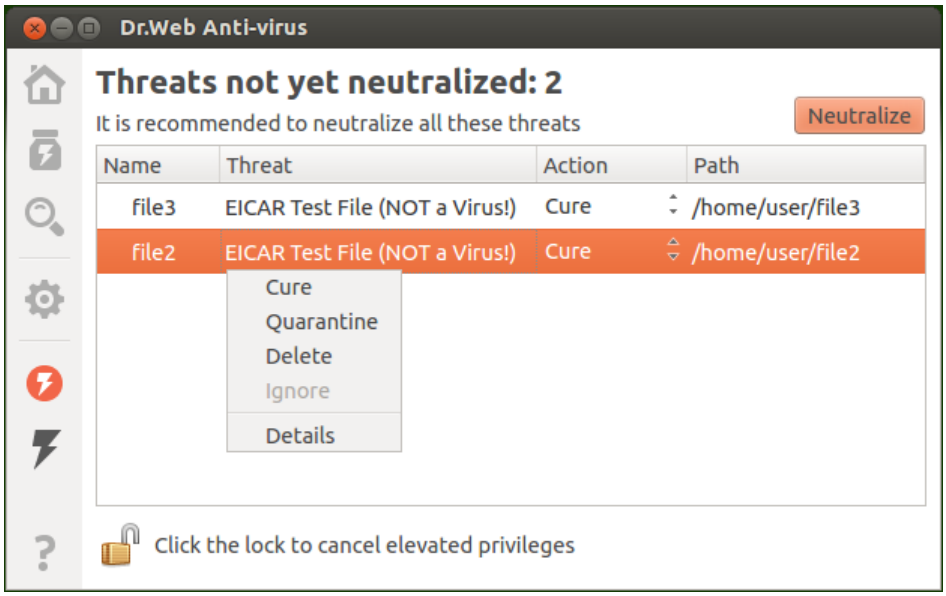
Configuring SpIDer Guard

SpIDer Guard settings are specified on the **SpIDer Guard** tab and on the **Exclusions** tab on the Settings page.

Viewing Detected Threats

The list of threats detected by **Scanner** and **SpIDer Guard** during the current **Anti-virus** session is displayed on the special window page which is available only if at least one threat is detected.

If threats are detected, you can open this page by clicking the button on the GUI navigation pane.



Picture 33. Page with listed threats

In the list, the following information is available for each detected threat:

- Name of the malicious object;
- Name of the threat (according to the **Doctor Web** classification);
- Action applied (or to be applied) to the threat;

- Path to the malicious object.

Neutralized threats display in the list as grayed out items.

Neutralizing Detected Threats

If some of the listed threats are not neutralized, the **Neutralize** button above the list becomes available. Once the button is clicked, actions specified in the corresponding **Action** fields are applied to the threats. If an attempt to neutralize a threat fails, the listed item is displayed red and an error message appears in the **Action** field.

By default, an action to be applied to a threat is selected according to the settings of the component which detected the threat. You can configure actions applied to threats of a certain type by **Scanner** and **SpIDer Guard**. For that purpose, open the corresponding tab on the Settings page and adjust the settings.

If it is necessary to apply an action which is different from the one specified in the settings, click the **Action** field and select the required action on the menu.

You can select multiple items in the threat list at a time. To do that, select the items with a mouse button while holding down CTRL and SHIFT keys.

- When you hold down a CTRL key, threats are selected one by one;
- When you hold down a SHIFT key, threats are selected contiguously.

After you select threats, you can apply a required action to them by right-clicking in the selected area and then clicking the required item on the displayed menu. The action selected on the menu is applied to all of the selected threats.

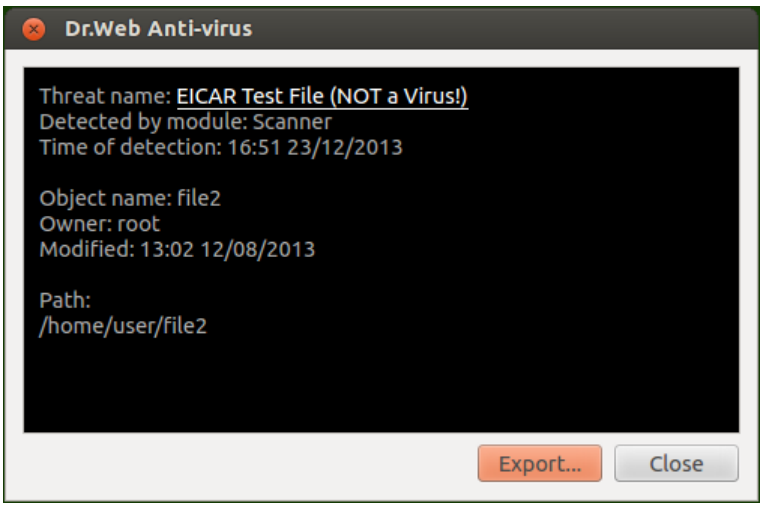
Note that

- If a threat is detected in a complex object (archive, email message, etc.), the selected action is applied to the container as a whole (and not to only the infected object);
- The **Cure** action can be applied not to all threat types;
- If a file contains only malicious content and has no useful content, effect of the **Cure** action is equal to the **Delete** action.

If required, elevate application privileges to enable successful neutralization of threats.

Viewing Information on Threats

For details on a detected threat, right click the item with information on the threat and then click **Details** on the displayed menu. After that, a window opens that contains detailed information on the threat and objects that contained the threat. To view information on multiple threats at a time, select the required items with a mouse button while holding a CTRL key.



Picture 34. Information on a threat

In this window, the following information is available:

- Name of the threat (according to the **Doctor Web** classification);
- Name of the **Dr.Web Anti-virus for Linux** component which detected the threat;
- Date and time of the detection;
- Information on the file system object where the threat was detected: object name, owner, date of the latest modification and path to the object in the file system.
- Last action applied to the threat and the result (if an option to apply actions to threat automatically is enabled for the component).

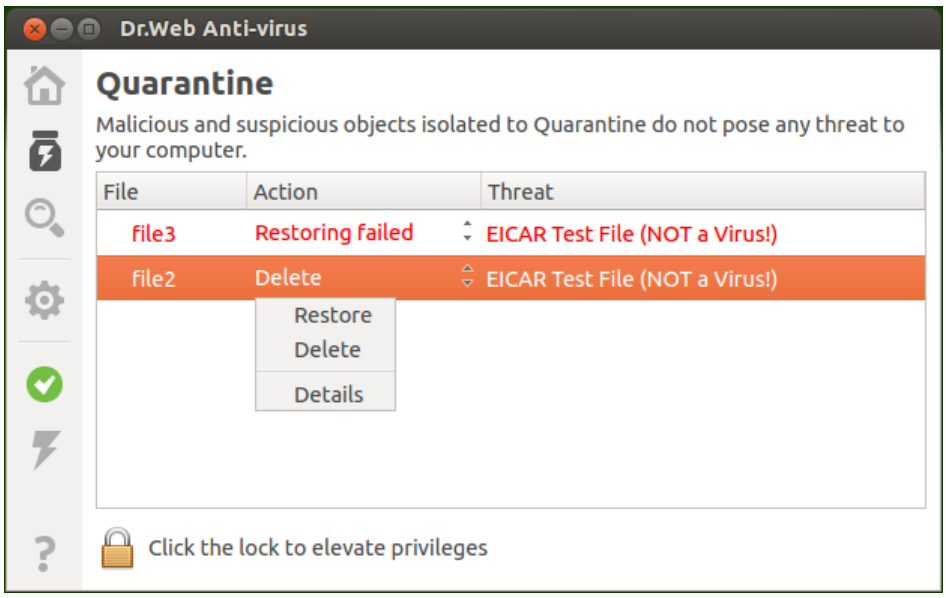
Clicking a threat name link opens a webpage with information on the threat in your browser (a threat name is a link to the official **Doctor Web** website; a valid Internet connection is required). You can also save the displayed information by clicking **Export...** (once you click the button, a window where you can select a file for saving opens).

To close the window with details on a threat and infected object, click **Close**.

Managing Quarantine

The list of files moved to **Quarantine** by **Dr.Web Anti-virus for Linux** components displays on a special window page.

To open the page where you can manage **Quarantine**, click the button on the navigation pane.



Picture 35. Quarantine management page

If **Quarantine** is not empty, the following information displays for each detected threat:

- Name of the infected object;
- Action to be applied to the quarantined object;
- Name of the threat (according to the **Doctor Web** classification).

Applying Actions to Isolated Objects

To apply an action to the quarantined object, right-click the line with the information on the isolated object and select a required action on the displayed menu. To apply an action to multiple objects, select them with the mouse button holding down a CTRL or SHIFT keys.

- When you hold down a CTRL key, isolated objects are selected by ones;
- When you hold down a SHIFT key, isolated objects are selected contiguously.

The following actions are available for isolated objects:

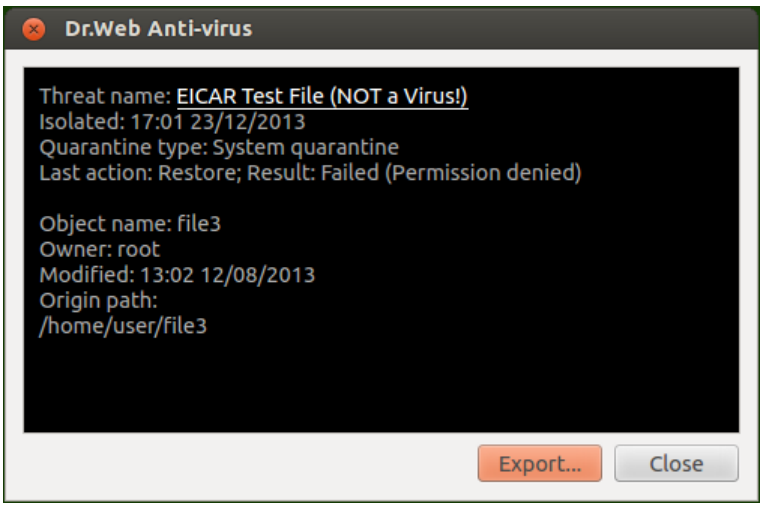
- **Restore** – restore the isolated object to its original location;
- **Delete** – permanently delete the object.

If the selected action is successfully applied to the object, its record is deleted from the table. If an attempt to apply an action failed, the item in the quarantined object list is displayed red and an error message appears in the **Action** field.

If required, elevate application privileges to enable successful neutralization of threats.

Viewing Information on Isolated Objects

For details on an isolated object, right-click in the line with information on the object and then click **Details** on the displayed menu. After that, a window opens that contains detailed information on the quarantined object. To view information on multiple objects at a time, select the required items with a mouse button while holding a CTRL key.



Picture 36. Information on a quarantined object

The window displays the following information:

- Threat name (according to **Doctor Web** classification);
- Date and time of moving the object to **Quarantine**;
- Type of the **Quarantine** directory where the object was moved;
- Last action applied to the object and the action result;
- Name of the **Dr.Web Anti-virus for Linux** component which detected the threat;
- Details on the isolated object: object name, owner name, last modified date and path to the object in the file system.

Clicking a threat name link opens a webpage with information on the threat in your browser (a threat name is a link to the official **Doctor Web** website; a valid Internet connection is required). You can save the displayed information to the text file by clicking the **Export...** button (once the button is clicked, a file chooser window opens).

To close the window with detailed information on the object, click **Close**.

Updating Virus Databases

Periodic updates to virus databases and **Anti-virus** engine are downloaded and installed by **Updater** automatically. You can view status of virus databases and force a database update on a special page of the **Anti-virus** window. To open the page, click **Update** on the Main page or click on the navigation pane (the button is visible only if the update management page was already opened from the Main page).

Picture 37. Update management page

The page displays the following information:

- Virus database status.
- Information on the last update and time of the next scheduled update.

To force a database update, click **Update**. To close the update management page, click **Close**.

If **Dr.Web Anti-virus for Linux** is operating in Central protection mode and the central protection server disabled manual updates according to the security policy of the anti-virus network, the update management page can be blocked.

Configuring Updates

You can configure **Dr.Web Anti-virus for Linux** update settings on the Settings page on the **Main** tab.

License Manager

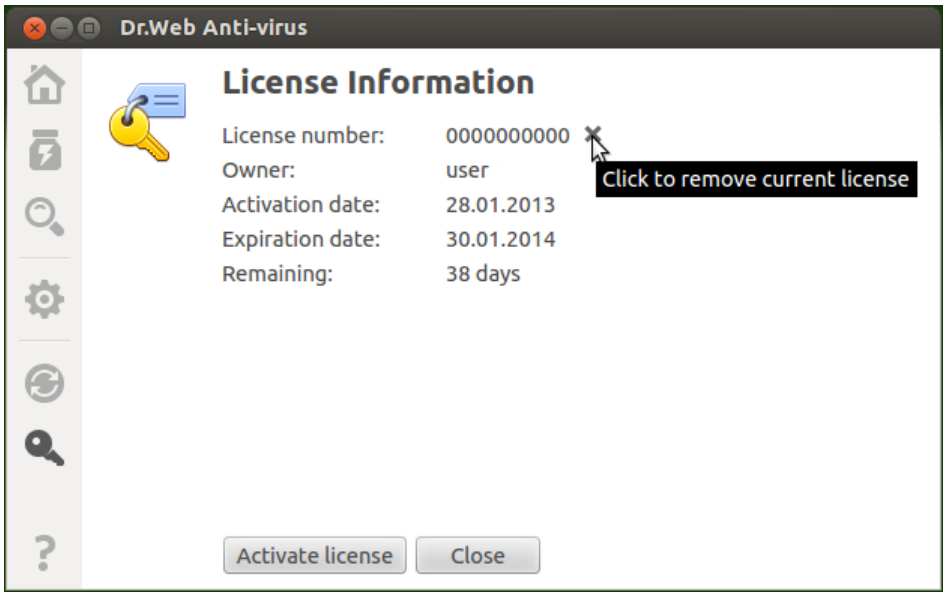
In graphics mode, **License manager** allows to view information on the current license issued for the **Dr.Web Anti-virus for Linux** user. License data is stored in a license key file that provides operation of **Anti-virus** on the user computer. If neither license key file nor demo key file is found on the computer, all **Dr.Web Anti-virus for Linux** functions (including file check, file system monitoring, virus database update) are blocked.

License Manager

License Manager page is available in the **Dr.Web Anti-virus for Linux** graphical inteface. To open the License manager page, click the **License** button on the Main page or click on the navigation pane (the button is visible only if the **License manager** page is already open from the Main page).

If a demo key file or license key file for **Dr.Web Anti-virus for Linux** to use is found, the **License Manager** start page displays license information including license number, license owner, and duration period. This information is retrieved from the corresponding key file.

The picture below shows appearance of the **License Manager** page.



Picture 38. License information page

To delete a license key file, click the cross icon next to the license number.

You can close **License Manager** at any stage by clicking the **Close** button at the bottom of the window. Once the button is clicked, the Main page of the **Dr.Web Anti-virus for Linux** opens.

License Activation

To activate a license via the **License Manager** and obtain the corresponding key file providing functionality of **Dr.Web Anti-virus for Linux** (which includes purchasing a new license or renewing the current one) or obtain a demo license, click **Activate license**. After that, the registration wizard opens. Note that the registration wizard also opens automatically when **Anti-virus** is first started after its installation.

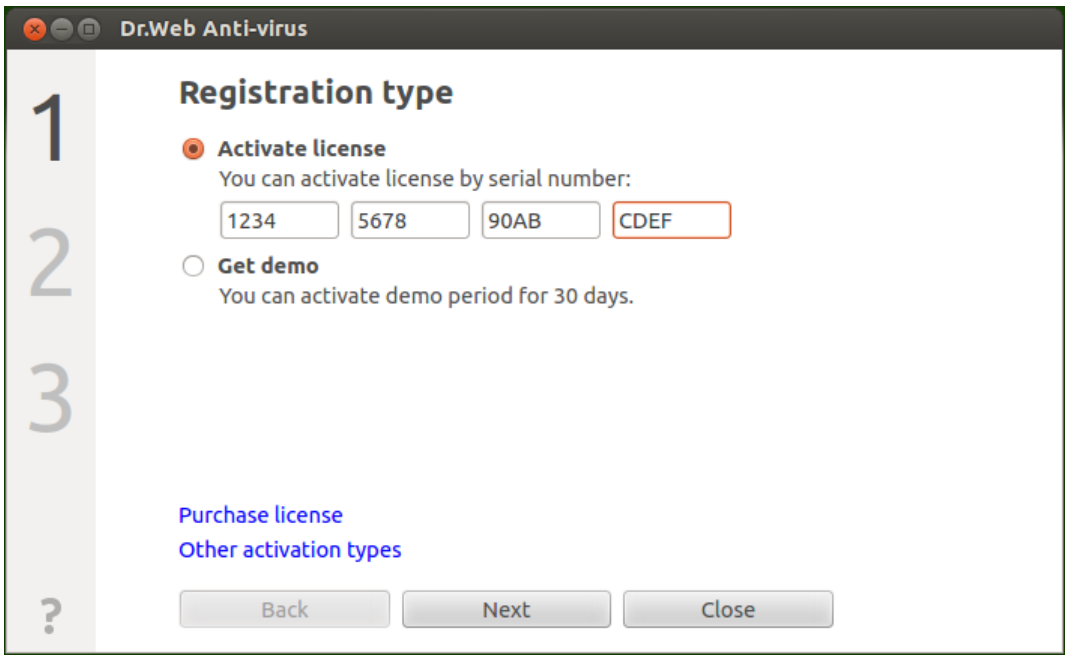
On the first step, select the activation type which can be one of the following:

1. Activation of license or demo period using a serial number;
2. Obtaining a demo period;
3. Installation of a key file obtained earlier;
4. Activation of **Anti-virus** via the central protection server.

To register a serial number and obtain a demo key file, a valid Internet connection is required.

1) Activation of license or demo period using a serial number

To activate a license or demo period using a serial number, select the **Activate license** item on the first step of the registration procedure. After that, enter the serial number in the four-segmented field and click **Next**.



Picture 39. Registration using a serial number

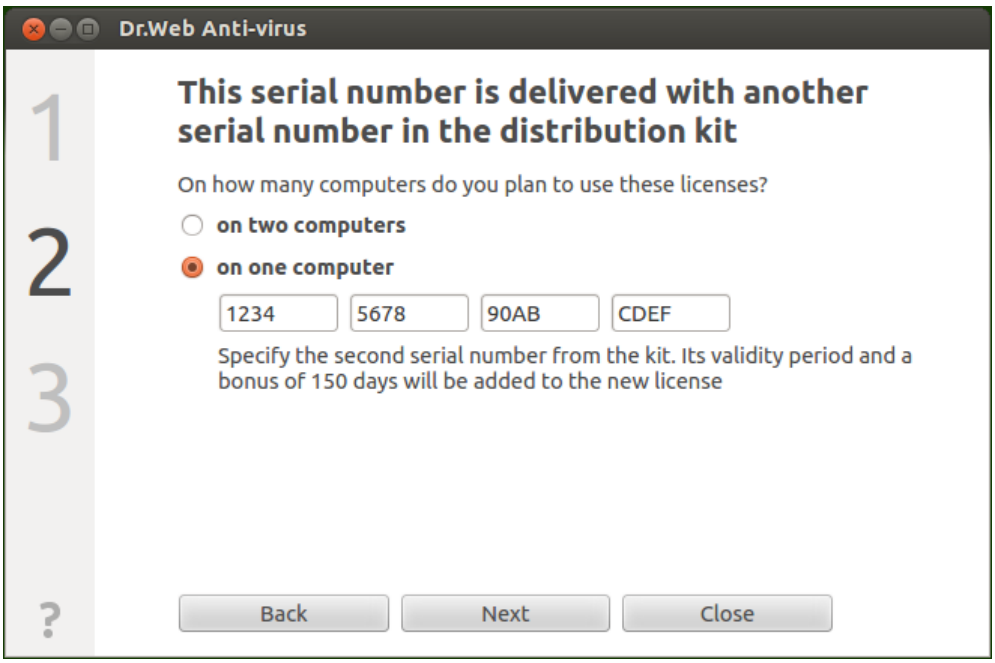
If you do not have a serial number or a valid key file, you can purchase license on the **Doctor Web** official website. To open the online store page, click **Purchase license.**

For information on other ways to purchase the license for **Dr.Web** products, refer to the Licensing section.

Once you click the **Next** button, connection to the **Doctor Web** registration server is established.

If the serial number, which you specified on the first step, was obtained from the **Doctor Web** website and issued for a three month's demo period, further steps are not required for its activation.

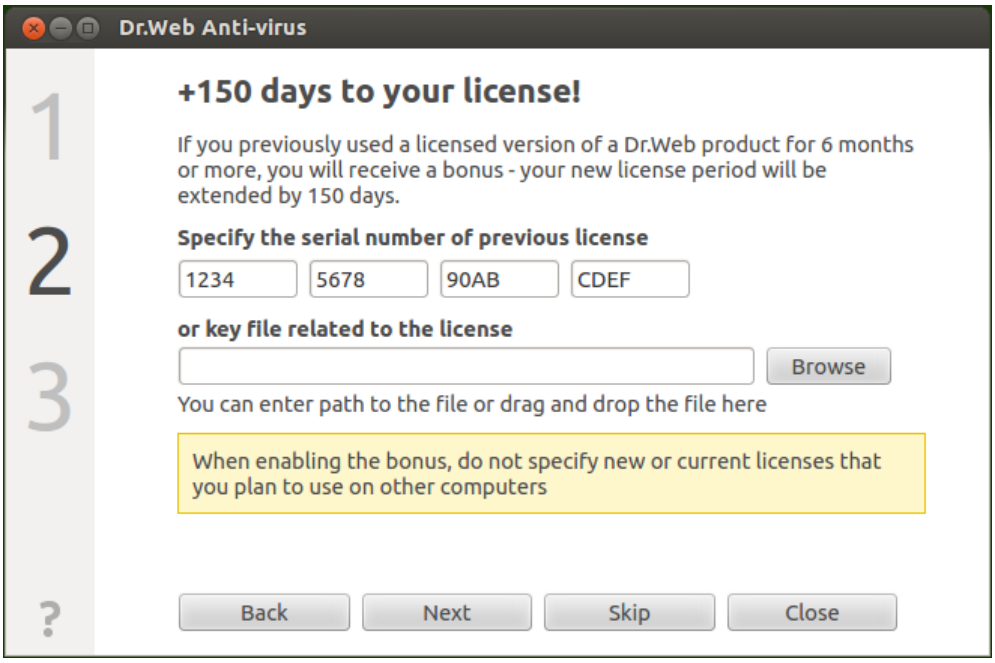
If the specified serial number corresponds to the license for using **Dr.Web Anti-virus for Linux** on two computers, you need to select on how many computers you would like to use the product. If you select **on two computers,** you can activate the second serial number on another computer and receive the second license key file. At that, the licenses are valid for the same period (for example, for one year). If you select **on one computer**, specify the second serial number in the appeared four-segmented field. In this case, you cannot register this serial number later on another computer (as well as use a copy of the license key file resulting from activation of a combined license), but the duration of the current license is doubled (for example, extended to two years if the license period is one year).



Picture 40. Selecting the number of computers

After you select the number of computers on which you would like to activate the license, click **Next**.

On this step, you are prompted to receive a bonus and extend the license period for 150 days. To enable the bonus, specify the previously purchased license if any.


Dr.Web Anti-virus
1
2
3
?
+150 days to your license!
If you previously used a licensed version of a Dr.Web product for 6 months or more, you will receive a bonus - your new license period will be extended by 150 days.
Specify the serial number of previous license
1234
5678
90AB
CDEF
or key file related to the license
Browse
You can enter path to the file or drag and drop the file here
When enabling the bonus, do not specify new or current licenses that you plan to use on other computers
Back
Next
Skip
Close

Picture 41. License renewal

If you specify a license which is not expired, the activated license period will be extended by the remaining period of the previous license and by the bonus of 150 days. You can skip this step (by clicking **Skip**), but in this case the remaining period of the previous license will be lost and the bonus will not be enabled. If you activate a license with two serial numbers, the bonus period will processed depending on the option you specified at the previous step.

- **On two computers**, and this computer is the first one. To enable the bonus of 150 days for

the first computer, specify the serial number of the previous license issued for this computer (if any). Do not specify the second serial number of the previous license here.

- **On two computers,** and this computer is the second one. To enable the bonus of 150 days for the second computer, specify either the serial number of the previous license issued for this computer (if any), or the serial number of the previous license issued for the first computer (if any).
- **On one computer.** In this case, not only the duration of the purchased licensed is doubled, but also the license period is extended for 150 days. Moreover, if you specify the previous license issued for the second computer, the doubled period of the new license will be extended by another 150 days (and by the remaining period of the previous license).

If you activate a special *renewal license* and click **Skip** at this step, the remaining period of the previous license will be lost and the validity period of the new license will be reduced by 150 days.

To specify the previous license, you can either enter its serial number in the corresponding field or specify its key file. To specify the key file, do one of the following:

- specify the file path in the entry filed
- specify the file via the standard file chooser by clicking the **Browse** button
- drag and drop the file from the file manager window to the window of the Registration wizard.

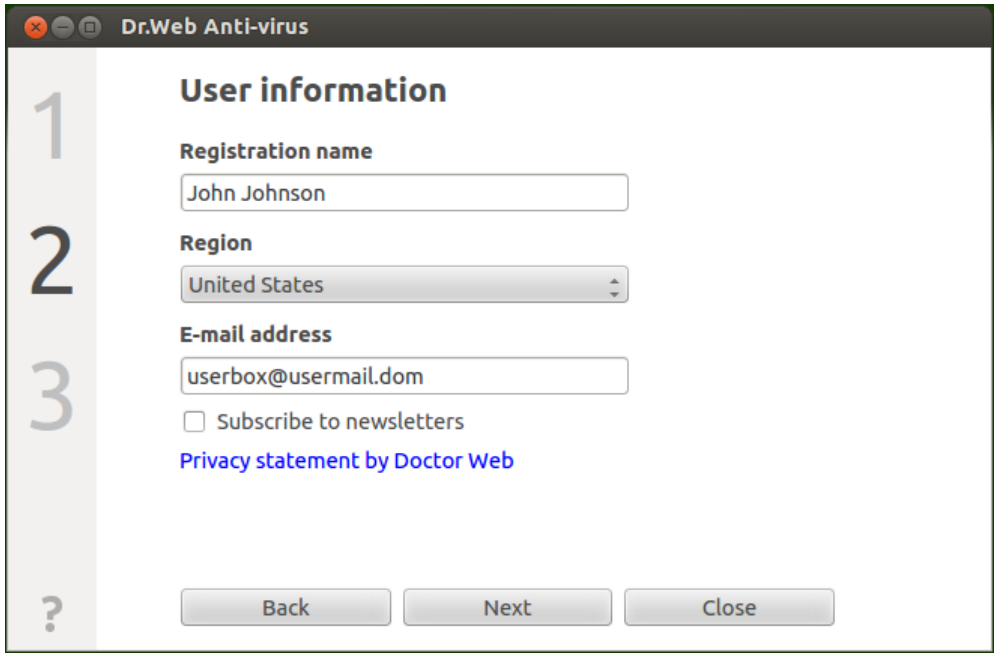
Note that you can specify the zip archive containing the key file without unpacking it.

To continue the registration, click **Next.**

On the next step, specify personal data including the following:

- Registration name;
- Your region (country), which is selected from the list;
- Correct email address.

All registration form fields are mandatory. Moreover, you can subscribe to **Doctor Web** newsletters (news emails are sent to the email address specified during the registration procedure) by selecting the corresponding checkbox.



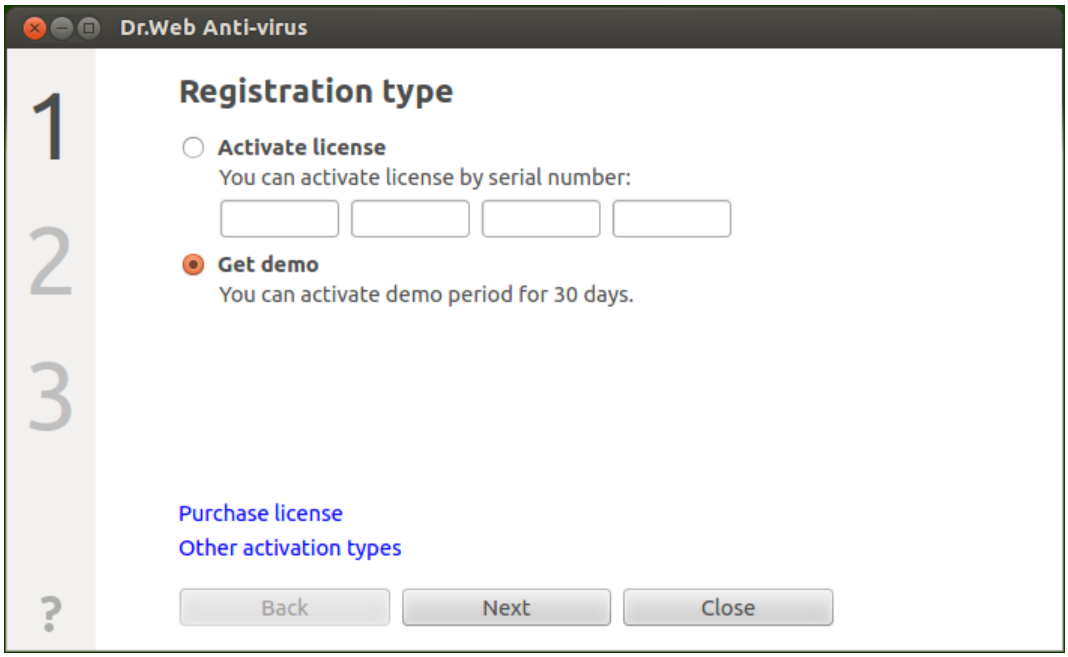
Picture 42. User information page

For **Doctor Web** privacy policy applied to personal user information, click the **Privacy statement by Doctor Web** link available on this page of the registration wizard (the webpage with the statement opens in your browser).

After all fields are filled in correctly, click the **Next** button to establish a server connection and obtain a license key file (note that clicking the button to continue registration means that you accept the privacy policy of **Doctor Web** applied to user personal information). If necessary, you can use the license key file on another computer after you remove it from this computer.

2) Obtaining a demo period

If you would like to activate a demo period that provides full functionality of **Dr.Web Anti-virus for Linux** components for a period of 30 days, select the **Get demo** item and click **Next**.

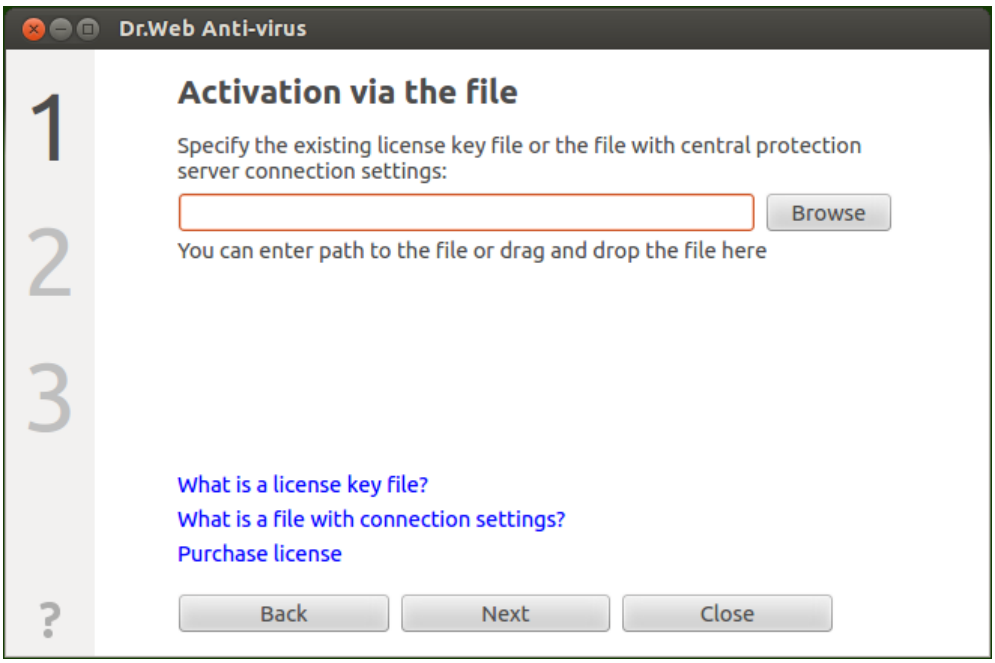


Picture 43. Obtaining a demo key file

When activating a demo period for 1 month, you do not need to provide your personal data. However, you can register on the official **Doctor Web** website and obtain a serial number for three month's demo period. Demo period for the same computer cannot be obtained more often than once a year. For details, refer to the Licensing section.

3) Installation of a key file obtained earlier

If you already have a valid license and the related key file (for example, obtained from **Doctor Web** or **Doctor Web** partners via email), you can activate **Dr.Web Anti-virus for Linux** by installing this key file. For that purpose, click **Other activation types** on the first step and specify the key file path in the displayed entry field and click **Next**.



Picture 44. Activation using the key file

To specify the key file, do one of the following:

- specify the file path in the entry filed
- specify the file via the standard file chooser by clicking the **Browse** button
- drag and drop the file from the file manager window to the window of the Registration wizard.

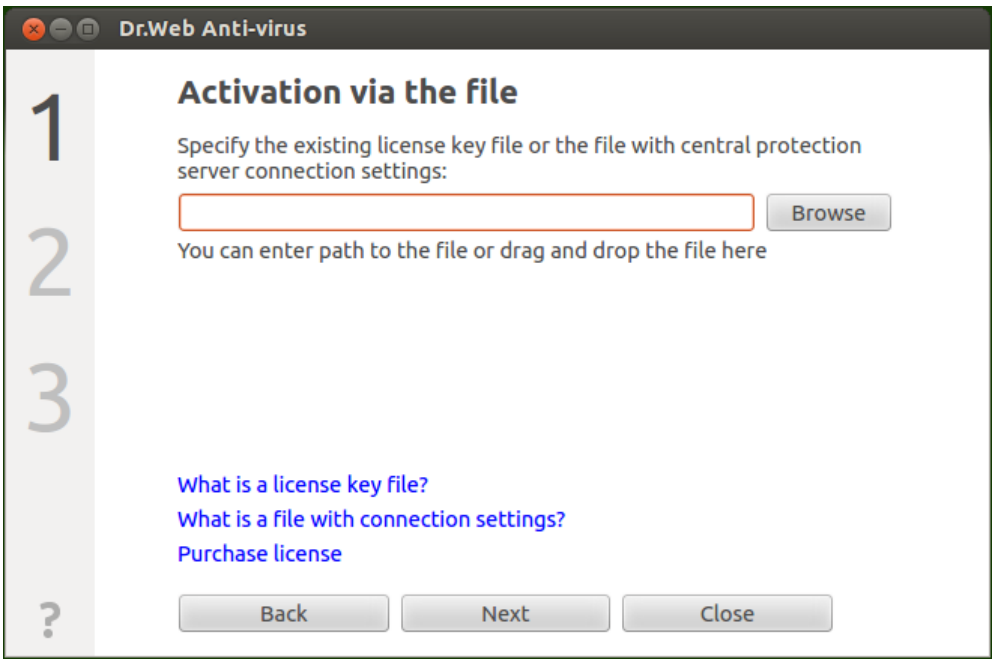
Note that you can specify the zip archive containing the key file without unpacking it.

After you specify the key file path (or the path to the archive containing the key file), click **Next** to install the key file automatically. If required, the key file is automatically unpacked and copied to the directory with **Anti-virus** files. An Internet connection is not required.

4) Activation of Anti-virus via the central protection server

You can activate your **Anti-virus** by connecting it to the central protection server which allows for central administration of the anti-virus network. In this case, the server generates a key file required for **Anti-virus** operation. Choose this activation type only if the provider or corporate network administrator delivered a special file which stores settings for connection of your **Anti-virus** to the central protection server.

To connect **Anti-virus** to the central protection server, click **Other activation types** on the first step, specify the path to the settings file and click **Next**.



Picture 45. Activation using the settings file

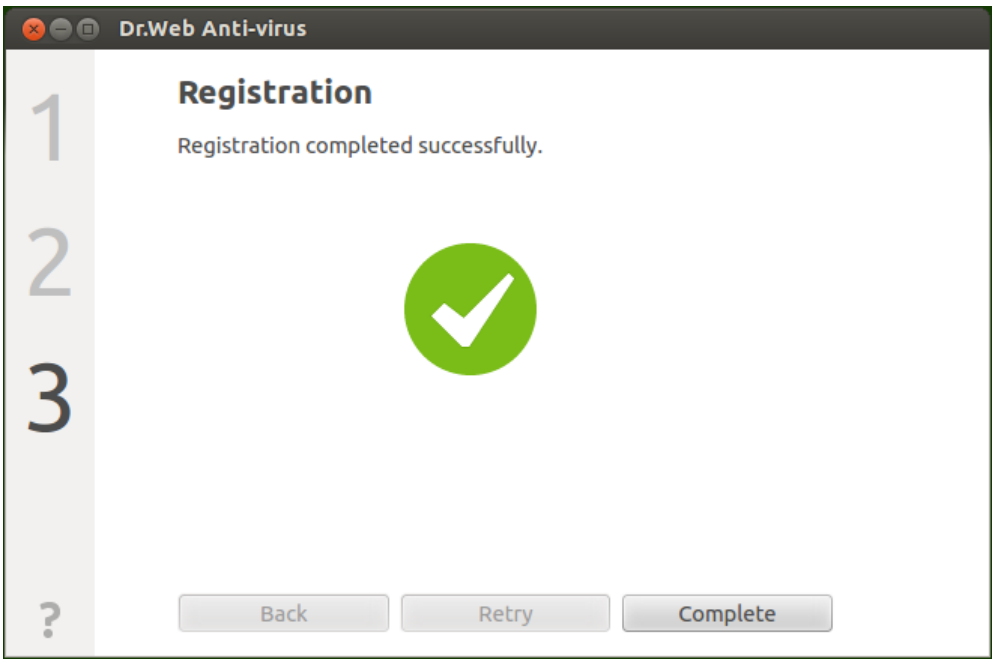
To specify the key file, do one of the following:

- specify the file path in the entry filed
- specify the file via the standard file chooser by clicking the **Browse** button
- drag and drop the file from the file manager window to the window of the Registration wizard.

Note that you can specify the zip archive containing the key file without unpacking it.

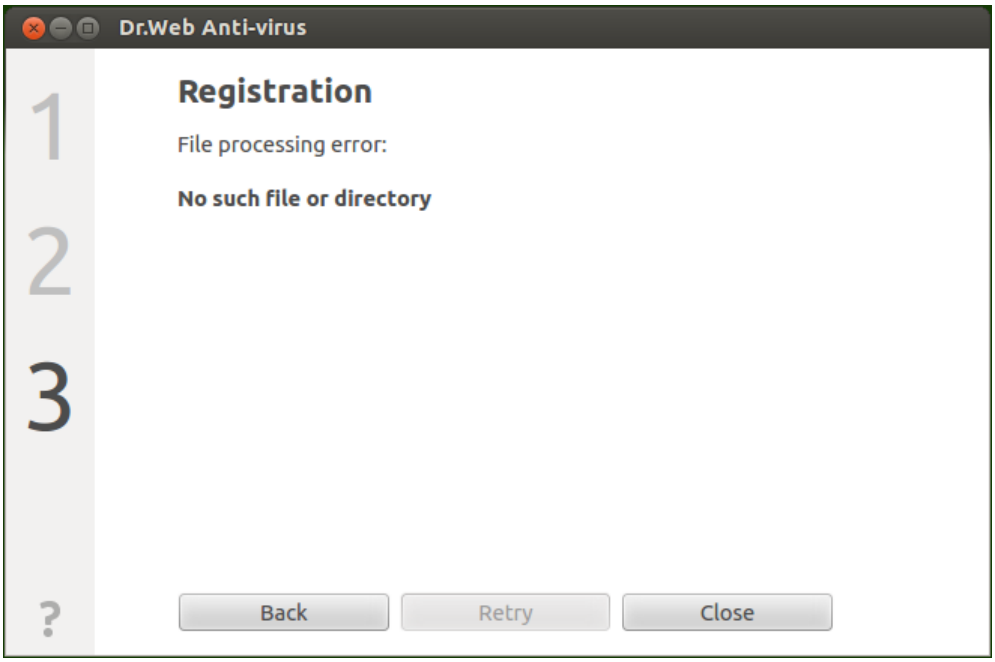
After you specify the path to the settings file (or the archive containing this file) click **Next** to establish connection to the central protection server (a network connection is required).

After the registration procedure completes (regardless of the selected activation type), the final page of the wizard with the corresponding notification displays. Click **Complete** to exit the wizard and open the Main page of the **Dr.Web Anti-virus for Linux**.



Picture 46. Successful registration notification

If an error occurs on any step of the procedure, a page with the corresponding notification and short error description displays. The picture below shows an example of such a page.



Picture 47. Error message

If an error occurs, you can return to the previous step and make corrections (for example, correct the serial number or specify the correct file path). To return to the previous step, click **Back**. If the error is caused due to a temporary problem (for example, temporary network failure), you can attempt to retry the operation by clicking **Retry**. If necessary, you can click **Close** to cancel the registration and exit the wizard. In this case, you need to retry the registration procedure later.

You can access the reference materials on any step by clicking . Moreover, some pages contain links to additional information.

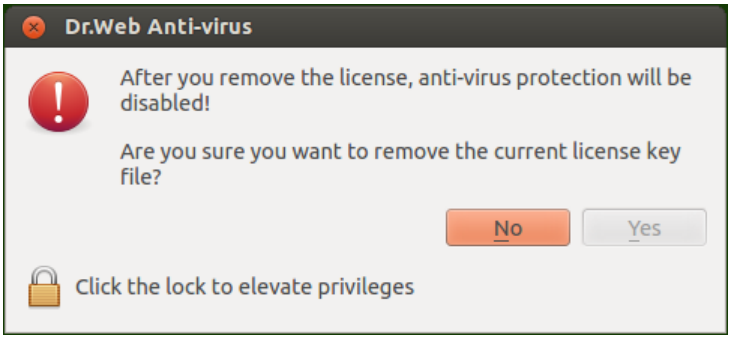
Note that upon activation of a new license and generation of a new key file, the previous key file, used by **Anti-virus,** is automatically saved as a backup copy to the `/etc/opt/drweb.com` directory.

If required, you can enable use of this key file again by installing it.

Deleting License Key File

If necessary (for example, if you decided to use **Dr.Web Anti-virus for Linux** on another computer), you can delete an installed license key file that manages **Anti-virus** operation. For that purpose, open the page with license information (the start page of **License manager**) and click the cross icon next to the number of the current license.

After that, confirm deletion of the license key file in the appeared window by clicking **Yes**. If you want to cancel the deletion, click **No**.


Dr.Web Anti-virus
After you remove the license, anti-virus protection will be disabled!
Are you sure you want to remove the current license key file?
No
Yes
Click the lock to elevate privileges

Picture 48. Confirmation dialog before deleting a license key file

To delete a license key file, the application must be started with superuser privileges. If the application does not have elevated permissions, the **Yes** button is unavailable on attempt to delete a key file. If required, you can elevate the privileges and, if the elevation succeeds, the **Yes** button becomes available.

Deletion of a license key file does not affect the license validity period. If the license is not expired, you can obtain a new key file for this license for the remaining period.

After a license key file is deleted, all anti-virus functions of **Dr.Web Anti-virus for Linux** (file scanning, virus database updating, file system monitoring) are blocked until a new license or demo period is activated.

Managing Application Privileges

Some operations with **Dr.Web Anti-virus for Linux** can be performed in graphics mode only if the application has elevated privileges that correspond to the superuser permissions. Among such actions are the following:

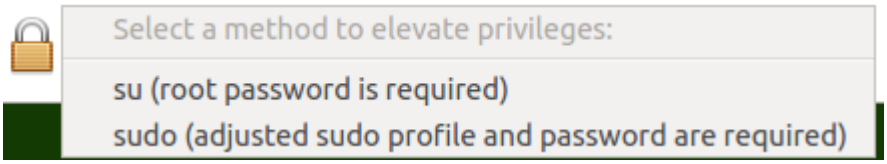
1. Management of objects moved to the system **Quarantine** (that is, to the non-user **Quarantine** directory);
2. Check of files and directories of other users (in particular, of superuser);
3. Disable **SpIDer Guard**;
4. Removal of a license key file, connection and disconnection from the central protection server.

All pages that provide for actions requiring superuser privileges contain a special button with a lock icon. The icon indicates whether or not the application has superuser privileges:

– Application does not have superuser privileges.
Click the icon to elevate the privileges.

– Application has superuser rights.
Click the icon to the lower privileges; that is, the application is running with the privileges of the user who started it.

On attempt to elevate privileges (i.e., once the lock icon is clicked) a pop-up menu that allows to select an elevation method appears.


Select a method to elevate privileges:
su (root password is required)
sudo (adjusted sudo profile and password are required)

Picture 49. Privilege elevation menu

The following two methods are available: using the **su** command (change the current user) and using the **sudo** command profile. Depending on the settings, a password dialog may appear after you select one of the methods. If so, enter the superuser password in the entry field. When lowering the privileges, password is not required.

To enable privilege elevation, the `su` or `sudo` utilities and the `xterm` terminal emulator are required.

Instead of this, it is recommended to install one of the utilities for elevating privileges from the desktop environment: `gksu`, `kdesu`, `beesu`, `gksudo`, `kdesudo`, `beesudo`.

If the application was started with superuser privileges, the icon of an open lock always displays unavailable. Thus, an option to lower the privileges is disabled.

Help and Reference

To access the Help file, click on the navigation pane.

Once you click the button, a pop-up menu with the following items appears:

- **Help** – opens the **Dr.Web Anti-virus for Linux** User manual;
- **Forum** – opens the webpage of the **Doctor Web** official forum (a valid Internet connection is required);
- **Technical support** – opens the **Doctor Web** technical support webpage (a valid Internet connection is required);
- **My Dr.Web** – opens your personal webpage on the **Doctor Web** official website (a valid Internet connection is required);
- **About** – opens a window showing information about your version of **Dr.Web Anti-virus for Linux**.

Configuring Operation Settings

On the settings page, you can configure the following application parameters:

- update period
- actions applied to detected threats (detected both by **Scanner** during scanning started on demand and by **SpIDer Guard**)
- list of objects to be excluded from **Scanner** and **SpIDer Guard** checks
- schedule to run periodic checks by **Scanner**
- protection mode (*Standalone*, *Central protection*).

To open the settings page, click on the navigation pane.

On the settings page, the following tabs are available:

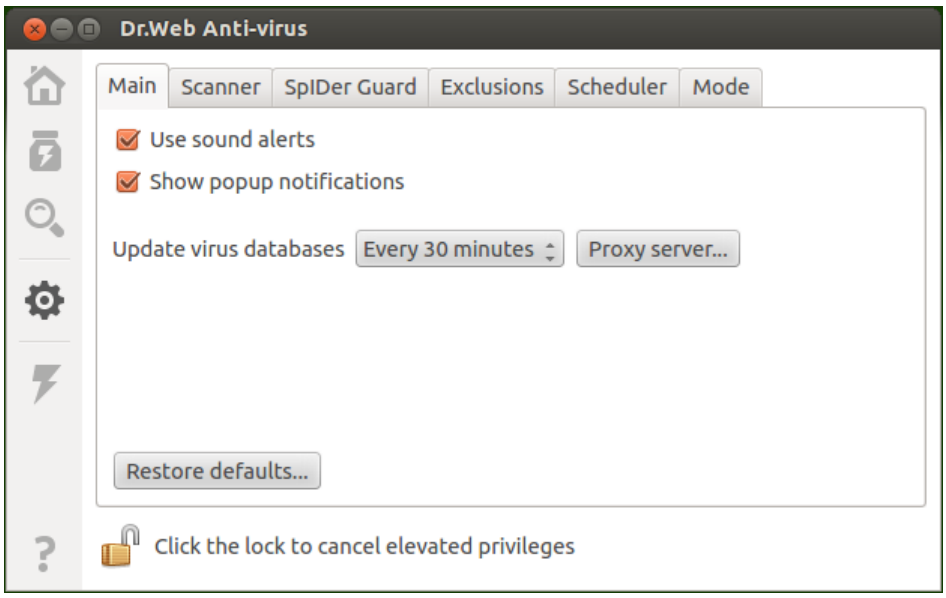
- Main – on this tab, you can configure notification settings and frequency of automatic updates.
- Scanner – on this tab, you can configure **Anti-virus** reaction to threats detected when scanning by **Scanner** on demand or as scheduled.
- SpIDer Guard – on this tab, you can configure **Anti-virus** reaction to threats detected by **SpIDer Guard.**
- Exclusions – on this tab, you can adjust the list of objects to be excluded from scanning on demand, from scanning started according to the schedule, or from **SpIDer Guard** checks.
- Scheduler – on this tab, you can configure the schedule to start scanning.
- Mode – on this tab, you can select the operation mode of **Dr.Web Anti-virus for Linux** (Standalone, Central protection).

All changes specified on these tabs are applied immediately.

Note that when **Dr.Web Anti-virus for Linux** is operating in Central protection mode, some of the settings can be not available.

Main Settings

On the **Main** tab, you can configure main application settings.



Picture 50. Main tab

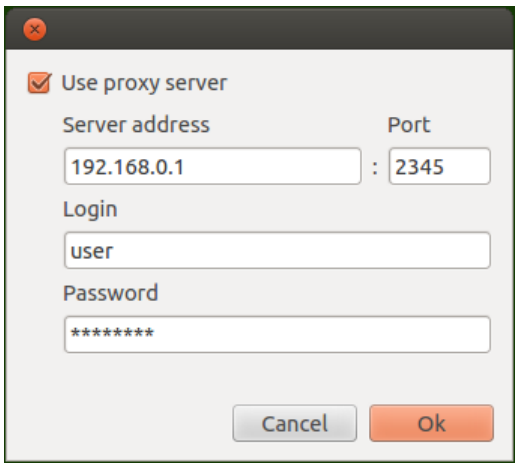
Option	Description
Use sound alerts	Select this checkbox if you want **Anti-virus** to use sound notifications on particular events, such as • detection of a threat (by both **Scanner** and **SpIDer Guard**) • scan error • others.
Show popup notifications	Select this checkbox if you want **Anti-virus** to show pop-up notifications on particular events, such as • threat detection • scan error • others.
Update virus databases	Select the frequency at which availability of updates to virus databases and to **Anti-virus** engine is checked by **Updater**.
Proxy server...	Click to configure proxy server settings for receiving updates (**Updater** uses a proxy server if contact to external servers is prevented by the network security policy).
Restore defaults...	Click to restore default values.

To manage update settings and restore defaults, the application must have superuser privileges. For details, refer to the Managing Application Privileges section.

Configuring Proxy Server for Updates

In the window with settings for **Updater** to use a proxy server, you can

- enable or disable use of the proxy server for receiving updates;
- specify address of the proxy sever used for receiving updates;
- specify the port to connect to the proxy server;
- specify the user name and password used for authentication on the proxy server.

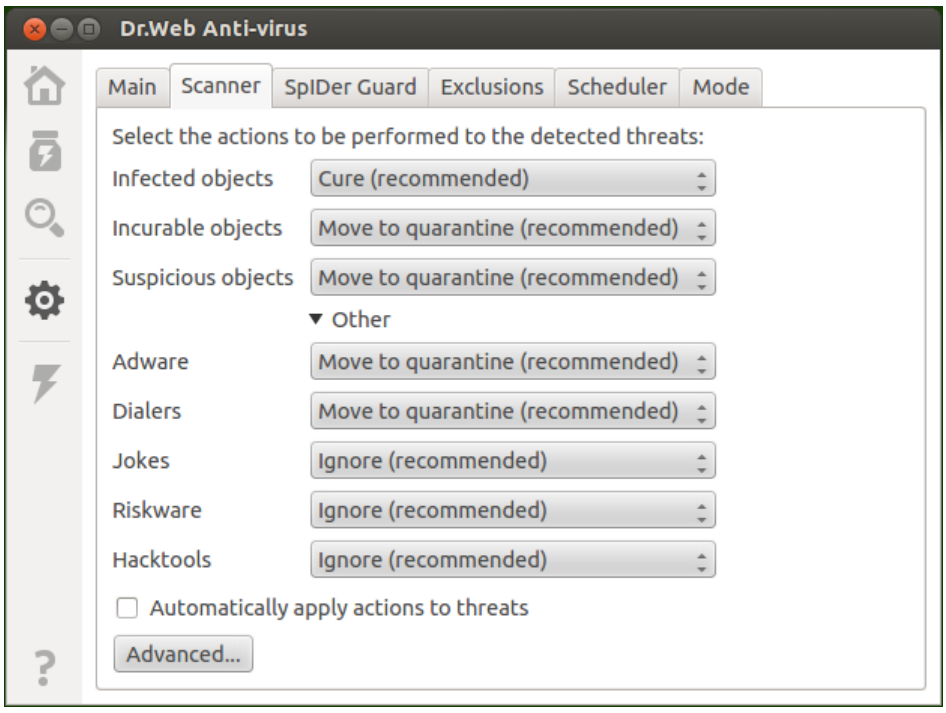


Picture 51. Proxy server settings

Click **OK** to save the changes and close the page or **Cancel** to reject them.

Scanner Settings

On the **Scanner** tab, you can specify actions that **Dr.Web Anti-virus for Linux** applies to threats detected when scanning files on user demand or as scheduled.



Picture 52. Scanner tab

In the drop-down lists select an action to be applied by **Dr.Web Anti-virus for Linux** to a threat of a certain type.

If you want **Anti-virus** to apply specified actions to malicious objects immediately upon threat detection, select the **Automatically apply actions to threats** checkbox. In this case, the user is notified on a neutralization event and information on the neutralized threat is added to the threat list). If the checkbox is not set, **Scanner** adds a detected threat to the list and the user manually selects an action to be applied.

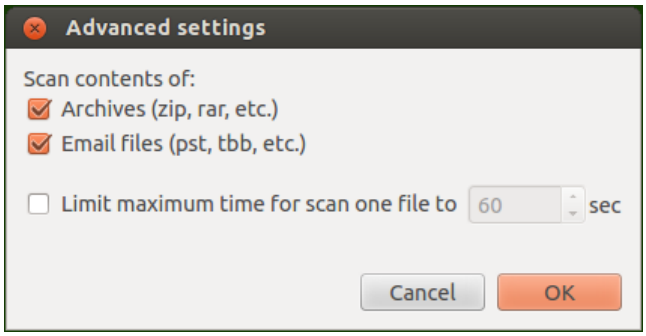
To ensure the highest security, it is recommended to select those reactions to threats that are indicated as recommended in the list and enable the **Automatically apply actions to threats** option.

To open a window with advanced scan settings, click the **Advanced...** button.

Advanced Scan Settings

In the window with advanced settings, you can configure parameters of **Scanner** operation, such as:

- Enable or disable scan contents of containers
  - archives;
  - mail files.
- Set maximum time to scan one file.



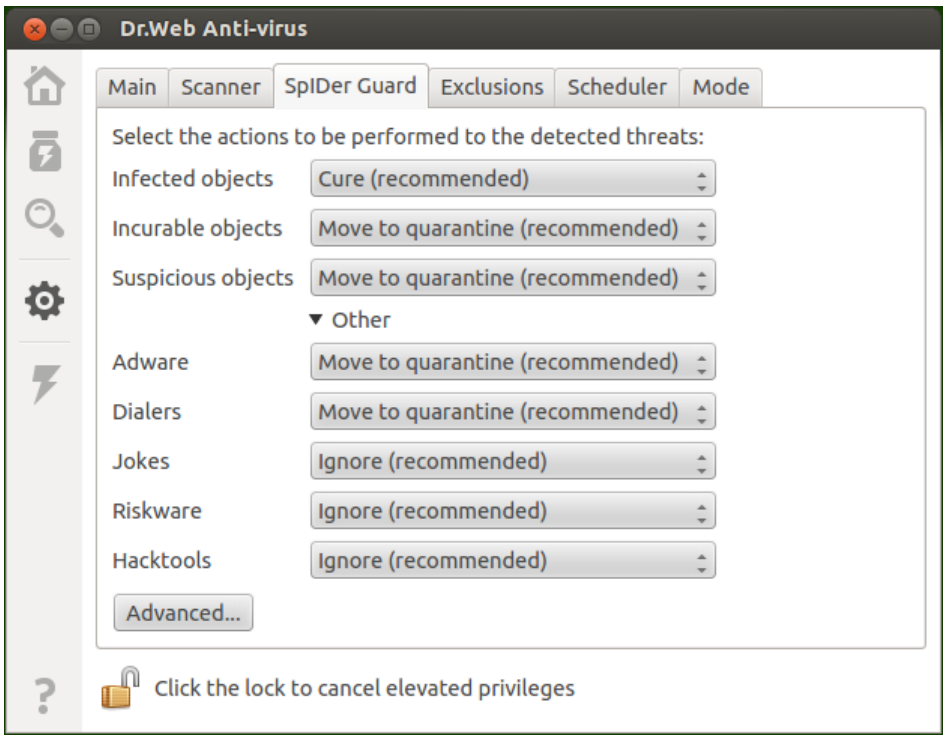
Picture 53. Advanced scan settings

If checkboxes are switched off, containers also will be scanned, but only as whole objects, without analysis of their internal structure.

Click **OK** to save the changes and close the window or **Cancel** to reject them.

SpIDer Guard Settings

On the **SpIDer Guard** tab, you can specify actions applied to threats detected by **SpIDer Guard** moritor.



Picture 54. SpIDer Guard tab

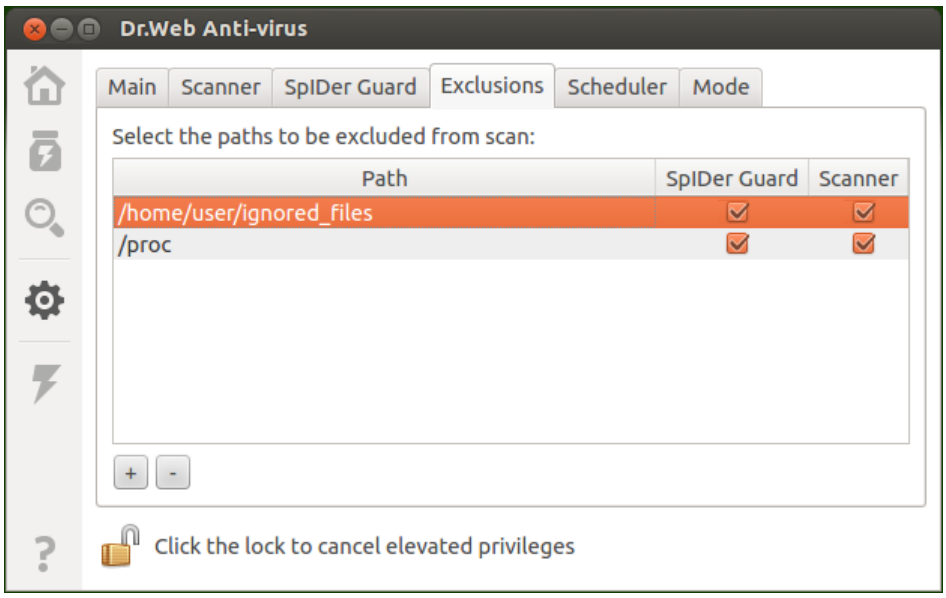
The options available on the tab are similar to those on the Scanner tab.

Adjustment of **SpIDer Guard** settings requires the application to have elevated privileges. For details, refer to the Application Rights Management section.

If **Anti-virus** is operating in Central protection mode, these settings are enabled in dependence on permissions are specified on the server.

Exclusions

On the **Exclusions** tab, you can specify paths to objects that you would like to exclude from scanning on user demand and/or as scheduled as well as adjust list of exclusions from **SpIDer Guard** checks.



Picture 55. Exclusions tab

You can add the same object to both lists of exclusions and disable its checks by **Scanner** (on demand and as scheduled) and by **SpIDer Guard**. If an object is added to an exclusion list, it is indicated with a flag in the corresponding column.

Adding and Removing Objects from Exclusion Lists

To add a listed object to the exclusions from **Scanner** or **SpIDer Guard** checks, select a respective checkbox in the object string. To remove an object from an exclusion list and enable object checks again, clear the corresponding checkbox in the object string.

To add a new object path to the list presented in this window, click the "+" button below the listed paths and select the new object in the appeared window. Besides that, you can add paths by dragging and dropping objects from the File Manager window.

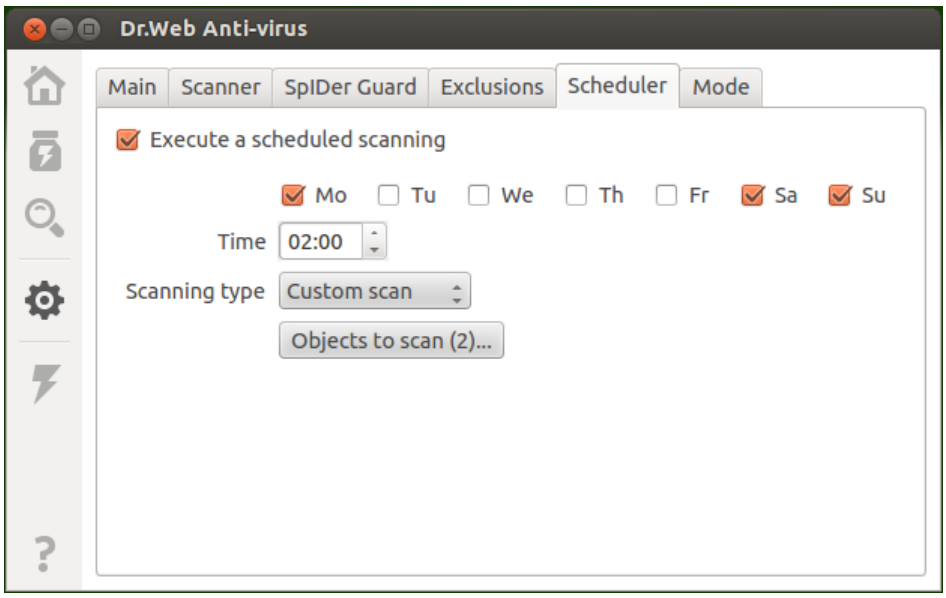
To remove an object path from the list, select the object string and click the "–" button below the listed paths.

Adding or removing an object from the exclusion list of **SpIDer Guard** requires the application to have elevated privileges. For details, refer to the Managing Application Privileges section.

Note that an object path cannot be removed if the object is added to the **SpIDer Guard** exclusion list and the application does not have permissions to adjust it.

Scheduler Settings

On the **Scheduler** tab, you can enable an option to scan objects automatically according to the schedule as well as specify this schedule and select the scanning type.



Picture 56. Scheduler tab

To enable automatic scheduled scans, select the **Execute a scheduled scanning** checkbox. In this case, **Dr.Web Anti-virus for Linux** creates a task for the **cron** job scheduler to periodically start scanning.

The **cron** job scheduler starts scanning at the specified intervals regardless of whether **Anti-virus** is started or not.

If **Anti-virus** is operating in Central protection mode and launching of scanning by user demand is prohibited on central protection server, the **Scanner** will not launch scannings even if they are scheduled.

Scanning started according to the schedule as well as scanning on demand is configured with the settings specified on the **Scanner** tab.

Configuring Scheduled Scanning

If scheduled scanning is enabled, you can configure the following parameters:

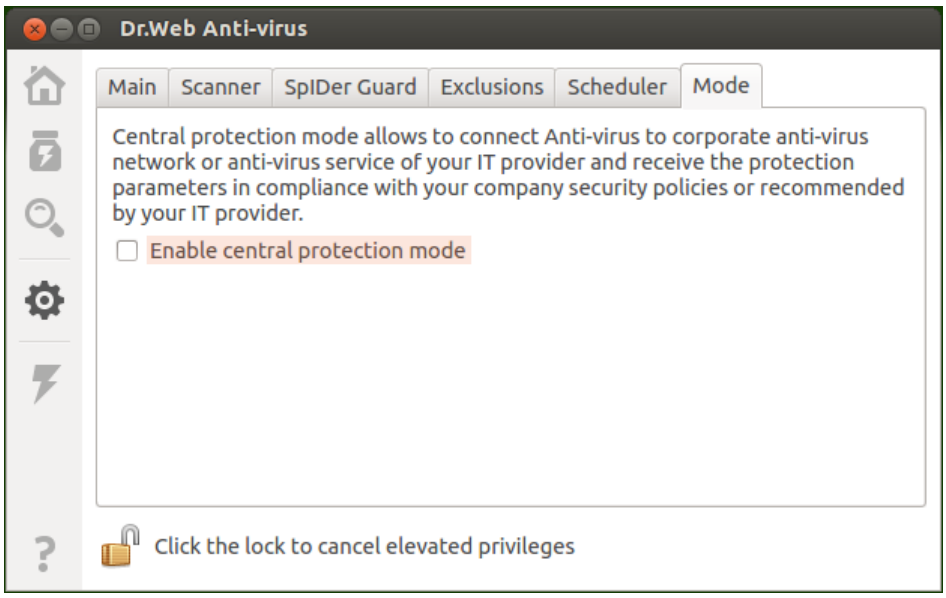
- days of week when scanning is to be started (by selecting the corresponding checkboxes);
- time (hours and minutes) when scanning is to be started;
- scan type (*Fast*, *Full*, or *Custom*).
- If you select *Custom scan* type, you can specify the list of objects to be scanned. For that purpose, click the **Objects to scan...** button (within the brackets number of selected objects is indicated).

  After that, select the necessary object in the appeared window which is similar to the file chooser for custom scanning on demand. You can add objects to the list either by clicking the "+" button or by dragging and dropping them from the File manager window.

To disable scheduled scanning, clear the **Execute a scheduled scanning** checkbox. The corresponding task is automatically removed from the **cron** task list.

Mode Settings

On the **Mode** tab, you can connect **Dr.Web Anti-virus for Linux** to the central protection server (by enabling Central protection mode) as well as disconnect from the central protection server (if so, **Dr.Web Anti-virus for Linux** is operating in Standalone mode).


Dr.Web Anti-virus
Main
Scanner
SpIDer Guard
Exclusions
Scheduler
Mode
Central protection mode allows to connect Anti-virus to corporate anti-virus network or anti-virus service of your IT provider and receive the protection parameters in compliance with your company security policies or recommended by your IT provider.
Enable central protection mode
Click the lock to cancel elevated privileges

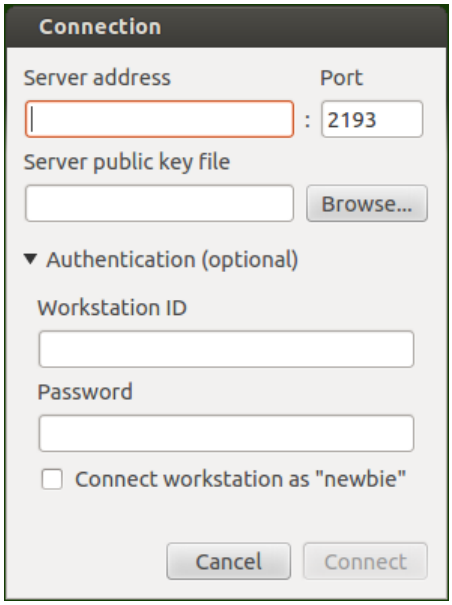
Picture 57. Mode tab

To connect **Dr.Web Anti-virus for Linux** to the central protection server or disconnect from that, use the corresponding checkbox.

To connect **Dr.Web Anti-virus for Linux** to the central protection server or disconnect from it, the application must have elevated privileges. For details, refer to the Managing Application Privileges section.

Connecting to Central Protection Server

On attempt to establish connection to the central protection server, a window with connection parameter appears.



Picture 58. Server connection dialog

To establish connection to the central protection server, specify the following parameters (provided by your network administrator or Internet service provider):

- address of the central protection server;
- port used when connecting to the central protection server;

- path to the file with the server public key.

Moreover, you can enter the identifier and password for the workstation to authenticate on the server (if known). Authentication will succeed only if the correct pair of identifier/password values is specified. If the fiields are empty, connection will be established only when approved on the server (automatically or by the anti-virus network administrator, depending on server settings).

You can also select the **Connect workstation as "newbie"** checkbox. If allowed on the server, a unique login/password pair will be automatically generated after the connection is approved. Note that if this checkbox is set, a new pair of values is generated even if the workstation already has an account on the server.

To connect to the server, specify all of the parameters, click **Connect** and wait for connection to be established. To close the window without establishing a server connection, click **Cancel**.

After you connected **Dr.Web Anti-virus for Linux** to the central protection server, **Anti-virus** is administered by the server until they are disconnected. In Central protection mode, a server connection is automatically established on every operating system startup. For details, refer to the Operation modes section.

Please note that in case if launching of scanning by user demand is prohibited on used central protection server, the Scan page of the **Anti-virus** window will be disabled. Moreover, in this case the **Scanner** will not launch scannings even if they are scheduled.

Advanced

Command Line Parameters

To start **Dr.Web Anti-virus for Linux** in graphics mode from the command line, the following command is used:

```
$ drweb-gui [options]
```

You can specify the following command options:

Short case	Full case	Arguments
-h	--help	
Description: Show information about supported command- line parameters and exit		
-v	--version	
Description: Show information on the module version and exit		
-d	--debug	
Description: Enable output of debug information when application is running.		
-t	--tray	
Description: Start the application minimized in tray.		

Example

```
$ drweb-gui --debug --tray
```

This command starts **Dr.Web Anti-virus for Linux** in graphics mode with enabled option to output debug information and the application window minimized in the tray.

Working from Command Line

You can manage operation of **Dr.Web Anti-virus for Linux** from the command line with the help of a special command-line tool - **drweb-ctl**.

You can do the following actions from the command line:

- Start scanning file system objects including boot records;
- Start updating virus databases;
- View and change parameters of **Anti-virus** configuration;
- View status of **Dr.Web Anti-virus for Linux** components and statistics on detected threats;
- View **Quarantine** and manage quarantined objects;
- Connect to the central protection server or disconnect from it.

To commands for **Anti-virus** management can have an effect if its service components are running (by default, the components are automatically started on operating system startup).

Note that some control commands require superuser privileges.

> To elevate privileges, use the **su** command (change the current user) or the **sudo** command (execute the specified command with other user privileges).

The **drweb-ctl** tool supports auto-completion of commands for managing **Anti-virus** operation if this option is enabled in the used command shell. If the command shell does not allow auto-completion, you can configure this option. For that purpose, refer to the instruction manual for the used operating system distribution.

Call Format

1. Format of the utility call

The call format for the command-line tool which manages **Dr.Web Anti-virus for Linux** operation is as follows:

```
$ drweb-ctl [<general options> | <command> [<argument>] [<command options>]]
```

where:

- `<general options>` – options that can be applied on startup when the command is not specified or can be applied for any command. Not mandatory for startup.
- **<command>** – command to be performed by **Anti-virus** (for example, start scanning, output the list of quarantined objects).
- `<argument>` – command argument. Depends on the specified command. Can be missing for certain commands.
- `<command options>` – options managing command operation. Depends on the command. Can be missing for certain commands.

2. General options

The following general options are available:

Option	Description
`-h`, `--help`	Show summary help information and exit. For information on a certain command, enter the following: **drweb-ctl** `-h` **<command>** or **drweb-ctl <command>** `-h`
`-v`, `--version`	Show information on the module version and exit
`-d`, `--debug`	Instructs to show debug information upon execution of the specified command. Has no effect if a command is not specified. To invoke a command, enter the following: **drweb-ctl** `-d` **<command>**

3. Commands

Commands to manage **Anti-virus** can be divided into the following groups:

- Anti-virus scanning commands;
- Commands to manage updates and operation in Central protection mode;
- Configuration management commands;
- Commands to manage detected threats and **Quarantine**;
- Information commands.

3.1. Anti-virus scanning commands

The following commands to manage anti-virus scanning are available:

Command	Description
scan <path>	**Function** Start checking the specified file or directory with **Scanner**. **Arguments** <path> – Path to the file or directory which is selected to be scanned. This argument can be missing if the --stdin or --stdin0 option is specified. To specify several files that satisfy a certain criterion, use the **find** utility (see the examples) and the --stdin or --stdin0 options. **Options** -a [--Autonomous] – Start a separate instance of **Anti-virus** engine and **Scanner** and terminate their operation after the scanning task completes. Note that threats detected during autonomous scanning are not displayed in the common threat list that is output by threats command (see below). --stdin – Get list of paths to scan from the standard input string (stdin). Paths in the list must be separated by the new line character ('\n'). --stdin0 – Get list of paths to scan from the standard input string (stdin). Paths in the list must be separated by the NUL character NUL ('\0'). Note that templates are not allowed when specifying paths for either of these options. Recommended usage of the --stdin and --stdin0 options is processing a path list (generated by an external utility, for example, **find**) in the **scan** command (see examples). --Report <BRIEF|DEBUG> – Specify the type of scanning results report. Possible values: • BRIEF – brief report. • DEBUG – detailed report. Default value: BRIEF --ScanTimeout <number> – Set the timeout value for scanning one file, in ms. If the value is set to 0, time to scan a file is not limited. Default value: 0 --PackerMaxLevel <number> – Set the maximum nesting level when scanning packed objects. If the value is set to 0, the nested objects are not checked. Default value: 8 --ArchiveMaxLevel <number> – Set the maximum level of nesting when scanning archives (zip, rar, etc.). If the value is set to 0, the nested objects are not checked. Default value: 8 --MailMaxLevel <number> – Set the maximum level of nesting when scanning email messages (pst, tbb, etc.). If the value is set to 0, the nested objects are not checked. Default value: 8 --ContainerMaxLevel <number> – Set the maximum level of nesting when scanning containers of other types (HTML and others). If the value is set to 0, the nested objects are not checked.

Command	Description
	Default values: 8 --MaxCompressionRatio <ratio> – Set the maximum compression ratio for scanned objects. The ratio must be at least equal to 2. Default value: 3000 --HeuristicAnalysis <On|Off> – Enable or disable *heuristics analysis*. Default value: On --OnKnownVirus <action> – Action applied to a threat detected using signature analysis. Allowed values: REPORT, CURE, QUARANTINE, DELETE. Default value: REPORT --OnIncurable <action> – Action applied on failure to cure a detected threat or if a threat is incurable. Allowed values: REPORT, QUARANTINE, DELETE. Default value: REPORT --OnSuspicious <action> – Action applied to a threat detected using heuristics analysis. Allowed values: REPORT, QUARANTINE, DELETE. Default value: REPORT --OnAdware <action> – Action applied to adware. Allowed values: REPORT, QUARANTINE, DELETE. Default values: REPORT --OnDialers <action> – Action applied to a dialer. Allowed values: REPORT, QUARANTINE, DELETE. Default values: REPORT --OnJokes <action> – Action applied to a joke program. Allowed values: REPORT, QUARANTINE, DELETE. Default values: REPORT --OnRiskware <action> – Action applied to a potentially dangerous program (riskware). Allowed values: REPORT, QUARANTINE, DELETE. Default values: REPORT --OnHacktools <action> – Action applied to a hacktool. Allowed values: REPORT, QUARANTINE, DELETE. Default values: REPORT
bootscan <disk drive> | ALL	**Function** Start checking boot records on the specified disks with **Scanner**. Both MBR and VBR records are scanned. **Arguments** <disk drive> – Path to a block file of the disk device boot record of which is to be scanned. If you specify ALL, all boot records of all available disks are scanned. Mandatory argument. **Options**

Command	Description
	`-a [--Autonomous]` – Start a separate instance of the **Anti-virus** engine and **Scanner** and terminate their operation after the scanning task completes. Note that threats detected during autonomous scanning are not displayed in the common threat list that is output by `threats` command (see below). `--Report <BRIEF|DEBUG>` – Specify the type of scanning results report. Possible values: • `BRIEF` – brief report. • `DEBUG` – detailed report. Default value: `BRIEF` `--ScanTimeout <number>` – Specify timeout to scan one file, in ms. If the value is set to 0, time to scan one file is not limited. Default value: 0 `--HeuristicAnalysis <On|Off>` – Enable or disable *heuristics analysis*. Default value: `On` `--Cure <Yes|No>` – Enable or disable attempts to cure detected threats. If the value is set to `no`, only notification is output. Default value: `No` `--ShellTrace` – Enable output of additional debug information when scanning a boot record.
procscan	**Function** Start checking executable files containing code of currently running processes with **Scanner**. **Arguments** No. **Options** `-a [--Autonomous]` – start a separate instance of the **Anti-virus** engine and **Scanner** and terminate their operation after the scanning task completes. Note that threats detected during autonomous scanning are not displayed in the common threat list that is output by `threats` command (see below). `--Report <BRIEF|DEBUG>` – specify the type of scanning report. Allowed values: • `BRIEF` – brief report. • `DEBUG` – detailed report. Default value: `BRIEF` `--ScanTimeout <number>` – Specify timeout to scan one file, in ms. If the value is set to 0, time to scan one file is not limited. Default value: 0 `--HeuristicAnalysis <On|Off>` – Enable or disable *heuristics analysis*. Default value: `On` `--PackerMaxLevel <number>` – Set the maximum nesting level when scanning packed objects. If the value is set to `0`, the nested objects are not checked . Default value: `8`

Command	Description
	`--OnKnownVirus <action>` – Action applied to a threat detected using signature analysis. Allowed values: `REPORT`, `CURE`, `QUARANTINE`, `DELETE`. Default value: `REPORT` `--OnIncurable <action>` – Action applied on failure to cure a detected threat or if a threat is incurable. Allowed values: `REPORT`, `QUARANTINE`, `DELETE`. Default value: `REPORT` `--OnSuspicious <action>` – Action applied to a threat detected using heuristics analysis. Allowed values: `REPORT`, `QUARANTINE`, `DELETE`. Default value: `REPORT` `--OnAdware <action>` – Action applied to adware. Allowed values: `REPORT`, `QUARANTINE`, `DELETE`. Default value: `REPORT` `--OnDialers <action>` – Action applied to dialers. Allowed values: `REPORT`, `QUARANTINE`, `DELETE`. Default value: `REPORT` `--OnJokes <action>` – Action applied to joke programs. Allowed values: `REPORT`, `QUARANTINE`, `DELETE`. Default value: `REPORT` `--OnRiskware <action>` – Action applied to potentially dangerous programs (riskware). Allowed values: `REPORT`, `QUARANTINE`, `DELETE`. Default value: `REPORT` `--OnHacktools <action>` – Action applied to hacktools. Allowed values: `REPORT`, `QUARANTINE`, `DELETE`. Default value: `REPORT` Note that if a threat is detected in an executable file, **Anti-virus** terminates all processes started from the file.

3.2. Commands to manage updates and operation in Central protection mode

The following commands for managing updates and operation in Central protection mode are available:

Command	Description
`update`	**Function** Instruct **Updater** to download and install updates to virus databases and components from **Dr.Web GUS** server or terminate an updating process if running. The command has no effect if **Anti-virus** is connected to the central protection server. **Arguments** No. **Options** `--Stop` – Terminate the currently performed updating process.
`esconnect` `<server>[:port]`	**Function**

Command	Description
	Connect **Dr.Web Anti-virus for Linux** to the specified central protection server (for example, **Dr.Web Enterprise Server**) or switch operation of **Dr.Web Anti-virus for Linux** to Mobile mode. For details on Anti-virus operation modes, refer to Operation modes. **Arguments** • `<server>` – IP address or network name of the host on which the central protection server is operating. The argument is mandatory. • `<port>` – Name of the port used by the central protection server. The argument is optional. Specify the argument only if the central protection server uses a non-standard port. **Options** `--Key <path>` – Path to the public key file of the central protection server to which **Anti-virus** is connected. Note that the option is mandatory. `--Login <ID>` – Login (workstation identifier) used for connection to the central protection server. `--Password <password>` – Password for connection to the central protection server. `--Compress <On|Off>` – Allow compression of transmitted data. Default value: `Off` `--Encrypt <On|Off>` – Allow encryption of transmitted data. Default value: `Off` `--Newbie` – Connect as a «newbie» (get a new account on the server). Note that this command requires `drweb-ctl` to be started with superuser privileges.
`esmobile`	**Function** Switch **Dr.Web Anti-virus for Linux** operation mode from Central protection to Mobile mode or vice versa. The command has no effect if **Anti-virus** is in autonomous mode. **Arguments** No. **Options** `--Disable` – Disable Mobile mode and attempt to connect to the central protection server.
`esdisconnect`	**Function** Disconnect **Dr.Web Anti-virus for Linux** from the central protection server and switch its operation to autonomous mode. The command has no effect if **Anti-virus** is in autonomous mode. **Arguments** No. **Options** No. Note that this command requires `drweb-ctl` to be started with superuser privileges.

3.3. Configuration management commands

The following commands to manage configuration are available:

Command	Description
`cfset`	**Function**

Command	Description
`<section>.<parameter> <value>`	Change the active value of the specified parameter in the current configuration. Note that an equal sign is not allowed. **Arguments** • `<section>` – Name of the configuration file where the parameter resides. The argument is mandatory. • `<parameter>` – Name of the parameter. The argument is mandatory. • `<value>` – New value that is to be assigned to the parameter. The argument is mandatory. The following format is used to specify the parameter value `<section>.<parameter> <value>` For description of the configuration file, refer to the `man` documentation `drweb.ini(5)`. **Options** `-a [--Add]` – Do not substitute the current parameter value but add the specified value to the list (allowed only for parameters that can have several values, specified as a list). `-e [--Erase]` – Do not substitute the current parameter value but remove the specified value from the list (allowed only for parameters that can have several values, specified as a list). `-r [--Reset]` – Reset the parameter value to the default. At that, `<value>` is not required in the command and is ignored if specified. Options are not mandatory. If they are not specified, the current parameter value (or the list of ones if several values are specified) are substituted with the specified value. For the `-r` option, a special syntax to invoke the **`cfset`** command is used: **`cfset`** `<section>.* -r` In this case, all parameters of the specified section are reset to defaults. Note that this command requires **`drweb-ctl`** to be started with superuser privileges.
`cfshow` `[<section> [.<parameter>]`	**Function** Output parameters of the current configuration. The command to output parameters is specified as follows `<section>.<parameter> = <value>`. Sections and parameters of non-installed components are not output. **Arguments** • `<section>` – Name of the configuration file section parameters of which are to be output. The argument is optional. If not specified, parameters of all configuration file sections are output. • `<parameters>` – Name of the output parameter. The argument is optional. If not specified, all parameters of the section are output. Otherwise, only this parameter is output. If a parameter is specified without the section name, all parameters with this name from all of the configuration file sections are output. **Options** `--Uncut` – Output all configuration parameters (not only those used with the currently installed set of components). If the option is not specified, only parameters used for configuration of the installed components are output. `--Ini` – Output parameter values in the INI file format: at first, the section name is specified in square brackets, then the section parameters listed as <parameter> = <value> pairs (one pair per line).

3.4. Commands to manage detected threats and Quarantine

The following commands for managing threats and **Quarantine** are available:

Command	Description
threats [<command> <object>]	**Function** Apply the specified action to detected threats by their identifiers. Type of the action is configured with the specified command option. If the action is not specified, output information on detected but not neutralized threats. **Arguments** No. **Options** -f [--Follow] – Wait for new messages on new threats and output the messages once they are received (interrupt waiting with ^C). --Cure <threat list> – Attempt to cure the listed threats (threat identifiers are specified as a comma-separated list). --Quarantine <threat list> – Move the listed threats to **Quarantine** (threat identifiers are specified as a comma-separated list) --Delete <threat list> – Delete the listed threats (threat identifiers are specified as a comma-separated list). --Ignore <threat list> – Ignore the listed threats (threat identifiers are specified as a comma-separated list). If it is required to apply the command to all detected threats, specify all instead of <threat list>. For example, the following command **drweb-ctl** threats --Quarantine all moves all detected malicious objects to **Quarantine**.
quarantine [<command> <object>]	**Function** Apply an action to the specified object in **Quarantine**. If not specified, the following information is output: object identifier in **Quarantine** and brief information on source files. **Arguments** No. **Options** --Delete <object> – Delete the specified object from **Quarantine**. Note that objects are deleted from **Quarantine** permanently. --Restore <object> – Restore the specified object from **Quarantine** to the original location. As an <object> specify the object identifier in **Quarantine**. To apply the command to all quarantined objects, specify all as an <object>. For example, the following command **drweb-ctl** quarantine --Restore all restores all objects from **Quarantine**.

3.5. Information Commands

The following information commands are available:

Command	Description
appinfo	**Function** Output information on active **Anti-virus** modules.

Command	Description
	Arguments No. **Options** `-f [--Follow]` – Wait for new messages on module status change and output them once such a message is received (interrupt waiting with **^C**).
baseinfo	**Function** Output information on the current version of the **Anti-virus** engine and status of virus databases. **Arguments** No. **Options** No.
license	**Function** Output information on the active license. **Arguments** No. **Options** No.

Example Usage

Example usage of the **drweb-ctl** command:

1) Start scanning of the `/home` directory with default parameters:

```
$ drweb-ctl scan /home
```

2) Scan paths listed in the `daily_scan` file (one path per line):

```
$ drweb-ctl scan --stdin < daily_scan
```

3) Start scanning the boot record on the **sda** disk:

```
$ drweb-ctl bootscan /dev/sda
```

4) Output all parameters from the `[Root]` section of the active configuration:

```
$ drweb-ctl cfshow Root
```

5) Set `'No'` as the **Start** parameter value in the `[LinuxSpider]` section (this parameter value disables **SpIDer Guard** – monitor of the file system in **Linux** OS):

```
# drweb-ctl cfset LinuxSpider.Start No
```

Note that superuser privileges are required to perform this action. To elevate the privileges, you can use the **sudo** command, as shown in the following example:

```
$ sudo drweb-ctl cfset LinuxSpider.Start No
```

Example usage of the **find** utility to select files for scanning (the **drweb-ctl** `scan --stdin` command):

1) Scan all files in all directories, starting from the root directory, on the same partition of the file system:

```
$ find / -xdev -type f | drweb-ctl scan --stdin
```

2) Scan all files in all directories, starting from the root directory, except files residing in the `/var/log/messages` and `/var/log/syslog` directories:

```
$ find / -type f ! -path /var/log/messages ! -path /var/log/syslog | drweb-ctl scan –stdin
```

3) Scan all files of the `root` user in all directories, starting from the root directory:

```
$ find / -type f -user root | drweb-ctl scan --stdin
```

4) Scan files of the `root` and `admin` users in all directories, starting from the root directory:

```
$ find / -type f \( -user root -o -user admin \) | drweb-ctl scan --stdin
```

5) Scan files of users with `UID` in the range `1000 – 1005` in all directories, starting from the root directory:

```
$ find / -type f -uid +999 -uid -1006 | drweb-ctl scan --stdin
```

6) Scan files in all directories, starting from the root directory, with a nesting level not more than five:

```
$ find / -maxdepth 5 -type f | drweb-ctl scan --stdin
```

7) Scan files in a root directory ignoring files in subdirectories:

```
$ find / -maxdepth 1 -type f | drweb-ctl scan --stdin
```

8) Scan files in all directories, starting from the root directory, with following all symbolic links:

```
$ find -L / -type f | drweb-ctl scan --stdin
```

9) Scan files in all directories, starting from the root directory, without following symbolic links:

```
$ find -P / -type f | drweb-ctl scan --stdin
```

10) Scan files created not later than July 3, 2013 in all directories, starting with the root directory:

```
$ find / -type f -newermt 2013-07-03 | drweb-ctl scan --stdin
```

Appendicies

Appendix A. Types of Computer Threats

Herein, the term "*threat*" is defined as any kind of software potentially or directly capable of inflicting damage to a computer or network and compromising the user's information or rights (that is, malicious and other unwanted software). In a wider sense, the term "threat" may be used to indicate any type of potential danger to the security of the computer or network (that is, vulnerabilities that can result in hacker attacks).

All of the program types stated below have the ability to endanger the user's data or confidentiality. Programs that do not conceal their presence (e.g. spam distribution software and various traffic analyzers) are usually not considered as computer threats, although they can become threats under certain circumstances.

In **Doctor Web** classification, all threats are divided according to the level of severity into two types:

- **Major threats** – classic computer threats that may perform destructive and illegal actions in the system on their own (erase or steal important data, crash networks, etc.). This type of computer threats consists of software that is traditionally referred to as malware (malicious software), that is, viruses, worms and Trojans.
- **Minor threats** – computer threats that are less dangerous than major threats, but may be used by a third person to perform malicious activity. Also, mere presence of minor threats in the system indicates its low protection level. Among IT security specialists this type of computer threats is sometimes referred to as grayware or PUP (potentially unwanted programs) and consists of the following program types: adware, dialers, jokes, riskware, hacktools.

Major threats

Computer Viruses

This type of computer threats is characterized by the ability to implement its code into other objects. Such implementation is called infection. In most cases, the infected file becomes a virus carrier itself and the implemented code does not necessarily match the original. Most viruses are intended to damage or destroy data in the system.

In **Doctor Web** classification, viruses are divided by the type of objects which they infect:

- **File viruses** infect files of the operating system (usually executable files and dynamic libraries) and activate upon launching of the infected file.
- **Macro-viruses** are viruses that infect documents used by Microsoft® Office and some other applications supporting macro commands (usually, written in Visual Basic). Macro commands are a type of implemented programs (macros) written in a fully functional programming language. For instance, in Microsoft® Word macros can automatically initiate upon opening (closing, saving, etc.) a document.
- **Script viruses** are created using script languages and usually infect other scripts (e.g. service files of an operating system). They are also able to infect other file formats that allow execution of scripts and thus take advantage of scripting vulnerabilities in Web applications.
- **Boot viruses** infect boot records of diskettes and partitions or master boot records of fixed disks. They require very little memory and remain ready to continue performing their tasks until a system roll-out, restart or shut-down occurs.

Most viruses have some kind of protection against detection. Protection methods are being constantly improved and ways to overcome them are constantly being developed. All viruses may also be classified according to the type of protection that they use:

- **Encrypted viruses** cipher their code upon every infection to hamper their detection in a file, boot sector or memory. All copies of such viruses contain only a small common code fragment (the decryption procedure) that can be used as a virus signature.
- **Polymorphic viruses** also encrypt there code, but besides that they also generate a special decryption procedure that is different in every copy of the virus. This means that such viruses do not have byte signatures.
- **Stealth viruses** perform certain actions to disguise their activity and thus conceal their presence in an infected object. Such viruses gather the characteristics of an object before infecting it and then plant these "dummy" characteristics that mislead the scanner searching for modified files.

Viruses can also be classified according to the programming language in which they are written (in most cases, it is Assembler, high-level programming languages, script languages, etc.) or according to affected operating systems.

Computer Worms

Worms have become a lot more widespread than viruses and other types of computer threats recently. Like viruses, they are able to reproduce themselves and spread their copies, but they do not infect other programs and files (that is, they do not need host files to spread). A worm infiltrates a computer from a worldwide or local network (usually via an attachment to an e-mail) and distributes its functional copies to other computers in the network. It can begin distributing itself either upon a user's action or in an automatic mode choosing which computers to attack.

Worms do not necessarily consist of only one file (the worm's body). Many of them have an infectious part (the shellcode) that loads into the main memory (RAM) and then downloads the worm's body as an executable file via the network. If only the shellcode is present in the system, the worm can be deleted by simply restarting the system (at which the RAM is erased and reset). However, if the worm's body infiltrates the computer, then only an anti-virus program can cope with it.

Worms have the ability to cripple entire networks even if they do not bear any payload (i.e. do not cause any direct damage) due to their intensive distribution.

In **Doctor Web** classification, worms are divided by the method of distribution:

- Net worms distribute their copies via various network and file-sharing protocols.
- Mail worms spread themselves using e-mail protocols (POP3, SMTP, etc.).
- Chat worms use protocols of popular messengers and chat programs (ICQ, IM, IRC, etc.).

Trojan Programs (Trojans)

This type of computer threats cannot reproduce itself or infect other programs. A Trojan substitutes a program that is used a lot and performs its functions (or imitates its operation). At the same time, it performs some malicious actions in the system (damages or deletes data, sends confidential information, etc.) or makes it possible for hacker to access the computer without permission, for example, to harm the computer of a third party.

A Trojan's masking and malicious facilities are similar to those of a virus. A Trojan may even be a component of a virus. However, most Trojans are distributed as separate executable files (through file-exchange servers, removable data carriers or e-mail attachments) that are launched by users or system tasks.

It is very hard to classify Trojans due to the fact that they are often distributed by viruses or worms and also because many malicious actions that can be performed by other types of threats are ascribed to Trojans only. Here are some Trojan types which are distinguished as separate classes in **Doctor Web**:

- **Backdoors** are Trojans that make it possible for an intruder to log on into the system or obtain privileged functions bypassing any existing access and security measures. Backdoors do not infect files, but they write themselves into the registry modifying the registry keys.
- **Rootkits** are used to intercept system functions of an operating system in order to conceal themselves. Besides, a rootkit can conceal processes of other programs (e.g. other threats), registry keys, folders and files. It can be distributed either as an independent program or as a component of another malicious program. There are two kinds of rootkits according to the mode of operation: User Mode Rootkits (UMR) that operate in user mode (intercept functions of the user mode libraries) and Kernel Mode Rootkits (KMR) that operate in kernel mode (intercept functions on the level of the system kernel, which makes it harder to detect).
- **Keyloggers** are used to log data that users enter by means of a keyboard. The aim of this is to steal personal information (i.e. network passwords, logins, credit card data, etc.).
- **Clickers** redirect hyperlinks to certain addresses in order to increase traffic of Web sites or perform DDoS attacks.
- **Proxy Trojans** provide anonymous Internet access through a victim's computer.

Trojans may also perform other malicious actions besides those stated above, for example, change the start page in a Web browser or delete certain files. However, other actions can also be performed by other types of threats (viruses and worms).

Minor Threats

Hacktools

Hacktools are programs designed to assist the intruder with hacking. The most common among them are port scanners that detect vulnerabilities in firewalls and other components of computer protection system. Besides hackers, such tools are used by administrators to check security of their networks. Occasionally, common software that can be used for hacking and various programs that use social engineering techniques are designated as among hacktools as well.

Adware

Usually, this term refers to a program code implemented into freeware programs that force display of advertisements to users. However, sometimes such codes can be distributed via other malicious programs and show advertisements in Web browsers. Many adware programs operate with data collected by spyware.

Jokes

Like adware, this type of minor threats can not be used to inflict any direct damage to the system. Joke programs usually just generate messages about errors that never occurred and threaten to perform actions that will lead to data loss. Their purpose is to frighten or annoy users.

Dialers

These are special programs that are designed to scan a range of telephone numbers and find those where a modem answers. These numbers are then used to mark up the price of telephoning facilities or to connect the user to expensive telephone services.

Riskware

These programs were not intended as computer threats, but can potentially cripple or be used to cripple system security due to certain features and, therefore, are classified as minor threats. Riskware programs are not only those that can accidentally damage or delete data, but also ones that can be used by crackers or some malicious programs to do harm to the system. Among such programs are various remote chat and administrative tools, FTP-servers, etc.

Suspicious Objects

These are possible computer threats detected by the heuristic analyzer. Such objects can potentially be any type of threat (even unknown to IT security specialists) or turn out safe in case of a false detection.

Suspicious objects should be sent for analysis to the **Doctor Web Virus Laboratory**.

Appendix B. Fighting Computer Threats

The **Dr.Web Anti-virus solutions** use several malicious software detection methods simultaneously, and that allows them to perform thorough checks on suspicious files and control software behavior.

Detection Methods

Signature analysis

The scans begin with *signature analysis* which is performed by comparison of file code segments to the known virus signatures. A *signature* is a finite continuous sequence of bytes which is necessary and sufficient to identify a specific virus. To reduce the size of the signature dictionary, the **Dr.Web Anti-virus solutions** use signature checksums instead of complete signature sequences. Checksums uniquely identify signatures, which preserves correctness of virus detection and neutralization. The **Dr.Web virus databases** are composed so that some entries can be used to detect not just specific viruses, but whole classes of threats.

Origins Tracing

On completion of signature analysis, the **Dr.Web Anti-virus solutions** use the unique **Origins Tracing™** method to detect new and modified viruses which use the known infection mechanisms. Thus, **Dr.Web** users are protected against such threats as notorious blackmailer **`Trojan.Encoder.18`** (also known as **`gpcode)`**. In addition to detection of new and modified viruses, the **Origins Tracing™** mechanism allows to considerably reduce the number of false triggering of the heuristics analyzer. Objects detected using the **Origins Tracing™** algorithm are indicated with the `.Origin` extension added to their names.

Execution emulation

The technology of program code emulation is used for detection of polymorphic and encrypted viruses, when the search against checksums cannot be applied directly, or is very difficult to be performed (due to the impossibility of building secure signatures). The method implies simulating the execution of an analyzed code by an *emulator* – a programming model of the processor and runtime environment. The emulator operates with protected memory area *(emulation buffer)*, in which execution of the analyzed program is modelled instruction by instruction. However, none of these instructions is actually executed by the CPU. When the emulator receives a file infected with a polymorphic virus, the result of the emulation is a decrypted virus body, which is then easily determined by searching against signature checksums.

Heuristic analysis

The detection method used by the heuristics analyzer is based on certain knowledge *(heuristics)* about certain features (attributes) than might be typical for the virus code itself, and vice versa, that are extremely rare in viruses. Each attribute has a weight coefficient which determines the level of its severity and reliability. The weight coefficient can be positive if the corresponding attribute is indicative of a malicious code or negative if the attribute is uncharacteristic of a computer threat. Depending on the sum weight of a file, the heuristics analyzer calculates the probability of unknown virus infection. If the threshold is exceeded, the heuristic analyzer generates the conclusion that the analyzed object is probably infected with an unknown virus.

The heuristics analyzer also uses the **FLY-CODE™** technology, which is a versatile algorithm for extracting files. The technology allows making heuristic assumptions about the presence of malicious objects in files compressed not only by packagers **Dr.Web** is aware of, but by also new, previously unexplored programs. While checking packed objects, **Dr.Web Anti-virus solutions** also use structural entropy analysis. The technology detects threats by arranging pieces of code; thus, one database entry allows identification of a substantial portion of threats packed with the same polymorphous packager.

As any system of hypothesis testing under uncertainty, the heuristics analyzer may commit type I or

type II errors (omit viruses or raise false alarms). Thus, objects detected by the heuristics analyzer are treated as "suspicious".

While performing any of the abovementioned checks, the **Dr.Web Anti-virus solutions** use the most recent information about known malicious software. As soon as experts of **Doctor Web Virus Laboratory** discover new threats, the update for virus signatures, behavior characteristics and attributes is issued. In some cases updates can be issued several times per hour. Therefore even if a brand new virus passes through the **Dr.Web** resident guards and penetrates the system, then after an update the virus is detected in the list of processes and neutralized.

Actions

To avert computer threats, **Dr.Web** products use a number of actions that can be applied to malicious objects. A user can leave the default settings, configure which actions to apply automatically, or choose actions manually upon every detection. Below is a list of possible actions:

- **Cure** is an action that can only be applied to major threats (viruses, worms and Trojans). It implies deletion of malicious code from infected objects as well as recovery of their structure and operability to the state in which it was before the infection if possible. Sometimes malicious objects are made of malicious code only (for example, Trojans or functional copies of computer worms) and for such objects to cure the system means to remove the whole object completely. Not all files infected by viruses can be cured, but curing algorithms evolve all the time.
- **Quarantine** (**Move to Quarantine**) is an action when the detected threat is moved to a special directory and isolated from the rest of the system. This action is preferable in cases when curing is impossible and for all suspicious objects. It is recommended to send copies of such files to the **Doctor Web Virus Laboratory** for analysis.
- **Delete** is the most effective action for averting computer threats. It can be applied to any type of computer threat. Note that deletion will sometimes be applied to certain objects for which the Cure action was selected. This will happen in cases if the object consists of only malicious code and have no useful information (for example, curing a computer worm implies deletion of all its functional copies).
- **Ignore** is an action applicable to minor threats only (that is, adware, dialers, jokes, hacktools and riskware) that instructs to skip the threat without performing any action or displaying information in report.
- **Report** means that no action is applied to the object and the threat is only listed in results report.

Appendix C. Contacting Support

Support is available to customers who have purchased a commercial version of **Dr.Web** products. Visit **Doctor Web Technical Support** website at http://support.drweb.com/.

If you encounter any issues installing or using company products, take advantage of the following **Doctor Web** support options:

- Download and review the latest manuals and guides at http://download.drweb.com/
- Read the frequently asked questions at http://support.drweb.com/
- Browse **Dr.Web Official Forum** at http://forum.drweb.com/

If you have not found solution for the problem, you can request direct assistance from **Doctor Web Technical Support** by filling in the web-from in the corresponding section of the support site at http://support.drweb.com/.

For regional office information, visit the **official Doctor Web website** at http://company.drweb.com/contacts/moscow.

Index

A
About product 8
Advanced 75
Application privileges 64

C
Central protection 72
Company 92
Components 10
Connection settings 18
Contacts 92
Context Application Menu 42
Conventions 6

E
EICAR 14
Exclusions 70

F
Features 8
Fighting Computer Threats 90
Files permissions 11
Forum 65
Functions 8

G
General settings 66
Get new version 19
Getting started 39
GUI 39
GUI command line arguments 75
GUI Quit 42
GUI start 42
GUI view 42

H
Help 65

I
Indicator 42
Intro 7

K
Key file 17
Key installation 17

L
License 15
License key file 17
License Manager 55
Licensing 15

M
Manual 65
Modules 10
Monitoring 49
Monitoring settings 69
My Dr.Web 65

N
Notifier 42

O
Operation modes 11

P
Protection mode settings 72
Purposes 8

Q
Quarantine 10
Quarantine management 52

R
Requirements 9

S
Scan 44
Scan Settings 68
Scan tasks 46
Scanner settings 68
Scheduler 71
Settings 66
SpIDer Guard 49
SpIDer Guard settings 69
Structure 10
Support 92

T
Testing Anti-virus 14
Threats detection 43

Index

Threats management 50
Tray Icon 42
Types of Computer Threats 86

U

Update 54
Upgrade 19

1992-2014, Doctor Web